

## PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

COMMUNICATION OF  
INTERNATIONAL APPLICATIONS  
(PCT Article 20)

Date of mailing:

30 November 2001 (30.11.01)

To:

Commissioner  
US Department of Commerce  
United States Patent and Trademark  
Office, PCT  
2011 South Clark Place Room  
CP2/5C24  
Arlington, VA 22202  
ETATS-UNIS D'AMERIQUE

in its capacity as designated Office

The International Bureau transmits herewith copies of the international applications having the following international application numbers and international publication numbers:

International application no.:

PCT/FR01/01564

International publication no.:

Best Available Copy

The International Bureau of WIPO  
34, chemin des Colombettes  
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra

Telephone No.: (41-22) 338.83.38

## TRAITÉ DE L'OPÉRATION EN MATIÈRE DE BREVETS

PCT  
PTO/PCT Rec'd 25 JAN 2002

AVIS INFORMANT LE DÉPOSANT DE LA  
COMMUNICATION DE LA DEMANDE  
INTERNATIONALE AUX OFFICES DÉSIGNÉS  
(règle 47.1.c), première phrase, du PCT)

Expéditeur: le BUREAU INTERNATIONAL de la

Propriété Intellectuelle

10 DEC. 2001 fedg

BULL S.A.

DENIS, Hervé  
Bull S.A.  
68, route de Versailles  
P.C.: 58D20  
F-78434 Louveciennes Cedex  
FRANCE

Date d'expédition (jour/mois/année)

30 novembre 2001 (30.11.01)

Référence du dossier du déposant ou du mandataire

PCT 3897 HD

## AVIS IMPORTANT

Demande internationale n°

PCT/FR01/01564

Date du dépôt international (jour/mois/année)

22 mai 2001 (22.05.01)

Date de priorité (jour/mois/année)

25 mai 2000 (25.05.00)

Déposant

HABERT, Michel

1. Il est notifié par la présente qu'à la date indiquée ci-dessus comme date d'expédition de cet avis, le Bureau international a communiqué, comme le prévoit l'article 20, la demande internationale aux offices désignés suivants:  
US

Conformément à la règle 47.1.c, troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communication de la demande internationale a bien eu lieu à la date d'expédition indiquée plus haut, et le déposant n'est pas tenu de remettre de copie de la demande internationale à l'office ou aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être effectuée à cette date:  
Aucun

La communication sera effectuée seulement sur demande de ces offices. De plus, le déposant n'est pas tenu de remettre de copie de la demande internationale aux offices en question (règle 49.1a-bis).

## RAPPEL CONCERNANT LE CHAPITRE II (article 31.2a) et règle 54.2)

Si le déposant souhaite reporter l'ouverture de la phase nationale jusqu'à 30 mois (ou plus pour ce qui concerne certains offices) à compter de la date de priorité, la demande d'examen préliminaire international doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 19 mois à compter de la date de priorité.

Il appartient exclusivement au déposant de veiller au respect du délai de 19 mois.

Il est à noter que seul un déposant qui est ressortissant d'un État contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international (actuellement, tous les États contractants du PCT sont liés par le chapitre II).

## RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1)

Si le déposant souhaite que la demande internationale procède en phase nationale, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu.

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase nationale, voir l'annexe du formulaire PCT/IB/301 (Notification de la réception de l'exemplaire original) et le Guide du déposant du PCT, volume II.

Bureau international de l'OMPI  
34, chemin des Colombettes  
1211 Genève 20, Suisse

Fonctionnaire autorisé

J. Zahra

n° de télécopieur (41-22) 740.14.35

n° de téléphone (41-22) 338.91.11

PCT

REQUÊTE

Le soussigné requiert que la présente demande internationale soit traitée conformément au Traité de coopération en matière de brevets.

Réervé à l'office récepteur

Demande internationale n°

Date du dépôt international

Nom de l'office récepteur et "Demande internationale PCT"

Référence du dossier du déposant ou du mandataire (facultatif)  
(12 caractères au maximum)

PCT 3897 HD

Cadre n° I TITRE DE L'INVENTION

Procédé et architecture de système de communication sécurisé entre deux entités connectées à un réseau de type internet, comprenant un segment de transmissions sans fil.

Cadre n° II DÉPOSANT

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)

HABERT Michel  
4, impasse J.H. Lartigue  
38120 SAINT-EGREVE  
FRANCE

Cette personne est aussi inventeur.

n° de téléphone

n° de télécopieur

n° de télimprimeur

Nationalité (nom de l'Etat) : FRANCE

Domicile (nom de l'Etat) : FRANCE

Cette personne est déposant pour :  tous les États désignés  tous les États désignés sauf les États-Unis d'Amérique  les États-Unis d'Amérique seulement  les États indiqués dans le cadre supplémentaire

Cadre n° III AUTRE(S) DÉPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)

Cette personne est :

déposant seulement

déposant et inventeur

inventeur seulement  
(Si cette case est cochée, ne pas remplir la suite.)

Nationalité (nom de l'Etat) :

Domicile (nom de l'Etat) :

Cette personne est déposant pour :  tous les États désignés  tous les États désignés sauf les États-Unis d'Amérique  les États-Unis d'Amérique seulement  les États indiqués dans le cadre supplémentaire

D'autres déposants ou inventeurs sont indiqués sur une feuille annexe.

Cadre n° IV MANDATAIRE OU REPRÉSENTANT COMMUN; OU ADRESSE POUR LA CORRESPONDANCE

La personne dont l'identité est donnée ci-dessous est/a été désignée pour agir au nom du ou des déposants auprès des autorités internationales compétentes, comme:

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays.)

mandataire

représentant commun

33 (1) 39.66.61.80

n° de télécopieur

33 (1) 39.66.61.73

n° de télimprimeur

DENIS Hervé

BULL S.A.

68, route de Versailles (P.C. : 58D20)

78434 LOUVECIENNES Cedex

France

Adresse pour la correspondance : cocher cette case lorsque aucun mandataire ni représentant commun n'est/n'a été désigné et que l'espace ci-dessus est utilisé pour indiquer une adresse spéciale à laquelle la correspondance doit être envoyée.

**Cadre n° V DÉSIGNATION D'ÉTATS**

Les désignations suivantes sont faites conformément à la règle 4.9.a) (cocher les cases appropriées; une au moins doit l'être) :

**Brevet régional**

**AP** Brevet ARIPO : GH Ghana, GM Gambie, KE Kenya, LS Lesotho, MW Malawi, MZ Mozambique, SD Soudan, SL Sierra Leone, SZ Swaziland, TZ République-Unie de Tanzanie, UG Ouganda, ZW Zimbabwe et tout autre Etat qui est un État contractant du Protocole de Harare et du PCT

**EA** Brevet eurasien : AM Arménie, AZ Azerbaïdjan, BY Bélarus, KG Kirghizistan, KZ Kazakhstan, MD République de Moldova, RU Fédération de Russie, TJ Tadjikistan, TM Turkménistan et tout autre État qui est un État contractant de la Convention sur le brevet eurasien et du PCT

**EP** Brevet européen : AT Autriche, BE Belgique, CH et LI Suisse et Liechtenstein, CY Chypre, DE Allemagne, DK Danemark, ES Espagne, FI Finlande, FR France, GB Royaume-Uni, GR Grèce, IE Irlande, IT Italie, LU Luxembourg, MC Monaco, NL Pays-Bas, PT Portugal, SE Suède et tout autre État qui est un État contractant de la Convention sur le brevet européen et du PCT

**OA** Brevet OAPI : BF Burkina Faso, BJ Bénin, CF République centrafricaine, CG Congo, CI Côte d'Ivoire, CM Cameroun, GA Gabon, GN Guinée, GW Guinée-Bissau, ML Mali, MR Mauritanie, NE Niger, SN Sénégal, TD Tchad, TG Togo et tout autre État qui est un État membre de l'OAPI et un État contractant du PCT (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée) . . . . .

**Brevet national (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée) :**

<input type="checkbox"/> <b>AE</b> Émirats arabes unis	<input type="checkbox"/> <b>LC</b> Sainte-Lucie
<input type="checkbox"/> <b>AG</b> Antigua-et-Barbuda	<input type="checkbox"/> <b>LK</b> Sri Lanka
<input type="checkbox"/> <b>AL</b> Albanie	<input type="checkbox"/> <b>LR</b> Liberia
<input type="checkbox"/> <b>AM</b> Arménie	<input type="checkbox"/> <b>LS</b> Lesotho
<input type="checkbox"/> <b>AT</b> Autriche	<input type="checkbox"/> <b>LT</b> Lituanie
<input type="checkbox"/> <b>AU</b> Australie	<input type="checkbox"/> <b>LU</b> Luxembourg
<input type="checkbox"/> <b>AZ</b> Azerbaïdjan	<input type="checkbox"/> <b>LV</b> Lettonie
<input type="checkbox"/> <b>BA</b> Bosnie-Herzégovine	<input type="checkbox"/> <b>MA</b> Maroc
<input type="checkbox"/> <b>BB</b> Barbade	<input type="checkbox"/> <b>MD</b> République de Moldova
<input type="checkbox"/> <b>BG</b> Bulgarie	<input type="checkbox"/> <b>MG</b> Madagascar
<input type="checkbox"/> <b>BR</b> Brésil	<input type="checkbox"/> <b>MK</b> Ex-République yougoslave de Macédoine
<input type="checkbox"/> <b>BY</b> Bélarus	<input type="checkbox"/> <b>MN</b> Mongolie
<input type="checkbox"/> <b>BZ</b> Belize	<input type="checkbox"/> <b>MW</b> Malawi
<input type="checkbox"/> <b>CA</b> Canada	<input type="checkbox"/> <b>MX</b> Mexique
<input type="checkbox"/> <b>CH et LI</b> Suisse et Liechtenstein	<input type="checkbox"/> <b>MZ</b> Mozambique
<input type="checkbox"/> <b>CN</b> Chine	<input type="checkbox"/> <b>NO</b> Norvège
<input type="checkbox"/> <b>CR</b> Costa Rica	<input type="checkbox"/> <b>NZ</b> Nouvelle-Zélande
<input type="checkbox"/> <b>CU</b> Cuba	<input type="checkbox"/> <b>PL</b> Pologne
<input type="checkbox"/> <b>CZ</b> République tchèque	<input type="checkbox"/> <b>PT</b> Portugal
<input type="checkbox"/> <b>DE</b> Allemagne	<input type="checkbox"/> <b>RO</b> Roumanie
<input type="checkbox"/> <b>DK</b> Danemark	<input type="checkbox"/> <b>RU</b> Fédération de Russie
<input type="checkbox"/> <b>DM</b> Dominique	<input type="checkbox"/> <b>SD</b> Soudan
<input type="checkbox"/> <b>DZ</b> Algérie	<input type="checkbox"/> <b>SE</b> Suède
<input type="checkbox"/> <b>EE</b> Estonie	<input type="checkbox"/> <b>SG</b> Singapour
<input type="checkbox"/> <b>ES</b> Espagne	<input type="checkbox"/> <b>SI</b> Slovénie
<input type="checkbox"/> <b>FI</b> Finlande	<input type="checkbox"/> <b>SK</b> Slovaquie
<input type="checkbox"/> <b>GB</b> Royaume-Uni	<input type="checkbox"/> <b>SL</b> Sierra Leone
<input type="checkbox"/> <b>GD</b> Grenade	<input type="checkbox"/> <b>TJ</b> Tadjikistan
<input type="checkbox"/> <b>GE</b> Géorgie	<input type="checkbox"/> <b>TM</b> Turkménistan
<input type="checkbox"/> <b>GH</b> Ghana	<input type="checkbox"/> <b>TR</b> Turquie
<input type="checkbox"/> <b>GM</b> Gambie	<input type="checkbox"/> <b>TT</b> Trinité-et-Tobago
<input type="checkbox"/> <b>HR</b> Croatie	<input type="checkbox"/> <b>TZ</b> République-Unie de Tanzanie
<input type="checkbox"/> <b>HU</b> Hongrie	<input type="checkbox"/> <b>UA</b> Ukraine
<input type="checkbox"/> <b>ID</b> Indonésie	<input type="checkbox"/> <b>UG</b> Ouganda
<input type="checkbox"/> <b>IL</b> Israël	<input checked="" type="checkbox"/> <b>US</b> États-Unis d'Amérique
<input type="checkbox"/> <b>IN</b> Inde	<input type="checkbox"/> <b>UZ</b> Ouzbékistan
<input type="checkbox"/> <b>IS</b> Islande	<input type="checkbox"/> <b>VN</b> Viet Nam
<input type="checkbox"/> <b>JP</b> Japon	<input type="checkbox"/> <b>YU</b> Yougoslavie
<input type="checkbox"/> <b>KE</b> Kenya	<input type="checkbox"/> <b>ZA</b> Afrique du Sud
<input type="checkbox"/> <b>KG</b> Kirghizistan	<input type="checkbox"/> <b>ZW</b> Zimbabwe
<input type="checkbox"/> <b>KP</b> République populaire démocratique de Corée	
<input type="checkbox"/> <b>KR</b> République de Corée	
<input type="checkbox"/> <b>KZ</b> Kazakhstan	

**Déclaration concernant les désignations de précaution :** outre les désignations faites ci-dessus, le déposant fait aussi conformément à la règle 4.9.b) toutes les désignations qui seraient autorisées en vertu du PCT, à l'exception de toute désignation indiquée dans le cadre supplémentaire comme étant exclue de la portée de cette déclaration. Le déposant déclare que ces désignations additionnelles sont faites sous réserve de confirmation et que toute désignation qui n'est pas confirmée avant l'expiration d'un délai de 15 mois à compter de la date de priorité doit être considérée comme retirée par le déposant à l'expiration de ce délai. (La confirmation (y compris les taxes) doit parvenir à l'office récepteur dans le délai de 15 mois.)

Case réservée pour la désignation d'États qui sont devenus parties au PCT après la publication de la présente feuille :

. . . . .

## Cadre n° VI REVENDICATIONS ET PRIORITÉ

d'autres revendications de priorité sont indiquées dans le cadre supplémentaire.

Date de dépôt de la demande antérieure (jour/mois/année)	Numéro de la demande antérieure	Lorsque la demande antérieure est une :		
		demande nationale : pays	demande régionale :* office régional	demande internationale : office récepteur
(1) 25 mai 2000 (25.05.2000)	0006693	FRANCE		
(2)				
(3)				

L'office récepteur est prié de préparer et de transmettre au Bureau international une copie certifiée conforme de la ou des demandes antérieures (seulement si la demande antérieure a été déposée auprès de l'office qui, aux fins de la présente demande internationale, est l'office récepteur) indiquées ci-dessus au(x) point(s) : 1

\* Si la demande antérieure est une demande ARIPO, il est obligatoire d'indiquer dans le cadre supplémentaire au moins un pays partie à la Convention de Paris pour la protection de la propriété industrielle pour lequel cette demande antérieure a été déposée (règle 4.10.b)ii)). Voir le cadre supplémentaire.

## Cadre n° VII ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Choix de l'administration chargée de la recherche internationale (ISA) (si plusieurs administrations chargées de la recherche internationale sont compétentes pour procéder à la recherche internationale, indiquer l'administration choisie; le code à deux lettres peut être utilisé) : ISA / FRANCE

Demande d'utilisation des résultats d'une recherche antérieure; mention de cette recherche (si une recherche antérieure a été effectuée par l'administration chargée de la recherche internationale ou demandée à cette dernière) :

Date (jour/mois/année) Numéro Pays (ou office régional)  
25.05.2000 0006693 FRANCE

## Cadre n° VIII BORDEREAU; LANGUE DE DÉPÔT

La présente demande internationale contient le nombre de feuillets suivant :

requête : 3  
description (sauf partie réservée au listage des séquences) : 21  
revendications : 5  
abrégé : 1  
dessins : 6  
partie de la description réservée au listage des séquences :  
Nombre total de feuillets : 36

Le ou les éléments cochés ci-après sont joints à la présente demande internationale :

- feuille de calcul des taxes
- pouvoir distinct signé
- copie du pouvoir général; numéro de référence, le cas échéant :
- explication de l'absence d'une signature
- document(s) de priorité indiqué(s) dans le cadre n° VI au(x) point(s) :
- traduction de la demande internationale en (langue) :
- indications séparées concernant des micro-organismes ou autre matériel biologique déposés
- listage des séquences de nucléotides ou d'acides aminés sous forme déchiffrable par ordinateur
- autres éléments (préciser) : Dessin abrégé

Figure des dessins qui doit accompagner l'abrégé : 9

Langue de dépôt de la demande internationale : Français

## Cadre n° IX SIGNATURE DU DÉPOSANT OU DU MANDATAIRE

À côté de chaque signature, indiquer le nom du signataire et, si cela n'apparaît pas clairement à la lecture de la requête, à quel titre l'intéressé signe.

Hervé DENIS (Mandataire Bull S.A.)

Réservé à l'office récepteur

1. Date effective de réception des pièces supposées constituer la demande internationale :	2. Dessins :
3. Date effective de réception, rectifiée en raison de la réception ultérieure, mais dans les délais, de documents ou de dessins complétant ce qui est supposé constituer la demande internationale :	<input type="checkbox"/> reçus : <input type="checkbox"/> non reçus :
4. Date de réception, dans les délais, des corrections demandées selon l'article 11.2) du PCT :	
5. Administration chargée de la recherche internationale (si plusieurs sont compétentes) : ISA /	6. <input type="checkbox"/> Transmission de la copie de recherche différée jusqu'au paiement de la taxe de recherche.

Réservé au Bureau international

Date de réception de l'exemplaire original par le Bureau international :

Direction de la  
Propriété Intellectuelle

# TRAITE DE L'OPERATION EN MATIERE DE BREVETS

- 6 AOUT 2001/edj

BULL S.A.

PCT

## NOTIFICATION DE LA RECEPTION DE L'EXEMPLAIRE ORIGINAL

(règle 24.2.a) du PCT

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

DENIS, Hervé  
Bull S.A.  
68, route de Versailles  
P.C.: 58D20  
F-78434 Louveciennes Cedex  
FRANCE

Date d'expédition (jour/mois/année) 30 juillet 2001 (30.07.01)	<b>NOTIFICATION IMPORTANTE</b>
Référence du dossier du déposant ou du mandataire PCT 3897 HD	Demande internationale n° PCT/FR01/01564

Il est notifié au déposant que le Bureau international a reçu l'exemplaire original de la demande internationale précisée ci-après.

Nom(s) du ou des déposants et de l'Etat ou des Etats pour lesquels ils sont déposants:

HABERT, Michel (tous les Etats désignés)

Date du dépôt international : 22 mai 2001 (22.05.01)

Date(s) de priorité revendiquée(s) : 25 mai 2000 (25.05.00)

Date de réception de l'exemplaire original par le Bureau international : 13 juillet 2001 (13.07.01)

Liste des offices désignés :

National : US

### ATTENTION

Le déposant doit soigneusement vérifier les indications figurant dans la présente notification. En cas de divergence entre ces indications et celles que contient la demande internationale, il doit aviser immédiatement le Bureau international.

En outre, l'attention du déposant est appelée sur les renseignements donnés dans l'annexe en ce qui concerne

- les délais dans lesquels doit être abordée la phase nationale
- la confirmation des désignations faites par mesure de précaution
- les exigences relatives aux documents de priorité.

Une copie de la présente notification est envoyée à l'office récepteur et à l'administration chargée de la recherche internationale.

Bureau international de l'OMPI  
34, chemin des Colombettes  
1211 Genève 20, Suisse

Fonctionnaire autorisé

Fiona DOHERTY

n° de télecopieur (41-22) 740.14.35

n° de téléphone (41-22) 338.83.38

## RENSEIGNEMENTS CONCERNANT LES DELAIS DANS LESQUELS DOIT ETRE ABORDEE LA PHASE NATIONALE

Il est rappelé au déposant qu'il doit aborder la "phase nationale" auprès de chacun des offices désignés indiqués sur la notification de la réception de l'exemplaire original (formulaire PCT/IB/301) en payant les taxes nationales et en remettant les traductions, telles qu'elles sont prescrites par les législations nationales.

Le délai d'accomplissement de ces actes de procédure est de **20 MOIS** à compter de la date de priorité ou, pour les Etats désignés qui ont été élus par le déposant dans une demande d'examen préliminaire international ou dans une élection ultérieure, de **30 MOIS** à compter de la date de priorité, à condition que cette élection ait été effectuée avant l'expiration du 19e mois à compter de la date de priorité. Certains offices désignés (ou élus) ont fixé des délais qui expirent au-delà de 20 ou 30 mois à compter de la date de priorité. D'autres offices accordent une prolongation des délais ou un délai de grâce, dans certains cas moyennant le paiement d'une taxe supplémentaire.

En plus de ces actes de procédure, le déposant devra dans certains cas satisfaire à d'autres exigences particulières applicables dans certains offices. Il appartient au déposant de veiller à remplir en temps voulu les conditions requises pour l'ouverture de la phase nationale. La majorité des offices désignés n'envoient pas de rappel à l'approche de la date limite pour aborder la phase nationale.

Des informations détaillées concernant les actes de procédure à accomplir pour aborder la phase nationale auprès de chaque office désigné, les délais applicables et la possibilité d'obtenir une prolongation des délais ou un délai de grâce et toutes autres conditions applicables figurent dans le volume II du Guide du déposant du PCT. Les exigences concernant le dépôt d'une demande d'examen préliminaire international sont exposées dans le chapitre IX du volume I du Guide du déposant du PCT.

GR et ES sont devenues liées par le chapitre II du PCT le 7 septembre 1996 et le 6 septembre 1997, respectivement, et peuvent donc être élues dans une demande d'examen préliminaire international ou dans une élection ultérieure présentée le 7 septembre 1996 (ou à une date postérieure) ou le 6 septembre 1997 (ou à une date postérieure), respectivement, quelle que soit la date de dépôt de la demande internationale (voir le second paragraphe, ci-dessus).

\*Veuillez noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

## CONFIRMATION DES DESIGNATIONS FAITES PAR MESURE DE PRECAUTION

Seules les désignations expresses faites dans la requête conformément à la règle 4.9.a) figurent dans la présente notification. Il est important de vérifier si ces désignations ont été faites correctement. Des erreurs dans les désignations peuvent être corrigées lorsque des désignations ont été faites par mesure de précaution en vertu de la règle 4.9.b). Toute désignation ainsi faite peut être confirmée conformément aux dispositions de la règle 4.9.c) avant l'expiration d'un délai de 15 mois à compter de la date de priorité. En l'absence de confirmation, une désignation faite par mesure de précaution sera considérée comme retirée par le déposant. Il ne sera adressé aucun rappel ni invitation. Pour confirmer une désignation, il faut déposer une déclaration précisant l'Etat désigné concerné (avec l'indication de la forme de protection ou de traitement souhaitée) et payer les taxes de désignation et de confirmation. La confirmation doit parvenir à l'office récepteur dans le délai de 15 mois.

## EXIGENCES RELATIVES AUX DOCUMENTS DE PRIORITE

Pour les déposants qui n'ont pas encore satisfait aux exigences relatives aux documents de priorité, il est rappelé ce qui suit.

Lorsque la priorité d'une demande nationale, régionale ou internationale antérieure est revendiquée, le déposant doit présenter une copie de cette demande antérieure, certifiée conforme par l'administration auprès de laquelle elle a été déposée ("document de priorité"), à l'office récepteur (qui la transmettra au Bureau international) ou directement au Bureau international, avant l'expiration d'un délai de 16 mois à compter de la date de priorité, étant entendu que tout document de priorité peut être présenté au Bureau international avant la date de publication de la demande internationale, auquel cas ce document sera réputé avoir été reçu par le Bureau international le dernier jour du délai de 16 mois (règle 17.1.a)).

Lorsque le document de priorité est délivré par l'office récepteur, le déposant peut, au lieu de présenter ce document, demander à l'office récepteur de le préparer et de le transmettre au Bureau international. La requête à cet effet doit être formulée avant l'expiration du délai de 16 mois et peut être soumise au paiement d'une taxe (règle 17.1.b)).

Si le document de priorité en question n'est pas fourni au Bureau international, ou si la demande adressée à l'office récepteur de préparer et de transmettre le document de priorité n'a pas été faite (et la taxe correspondante acquittée, le cas échéant) avant l'expiration du délai applicable mentionné aux paragraphes précédents, tout Etat désigné peut ne pas tenir compte de la revendication de priorité; toutefois, aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Lorsque plusieurs priorités sont revendiquées, la date de priorité à prendre en considération aux fins du calcul du délai de 16 mois est la date du dépôt de la demande la plus ancienne dont la priorité est revendiquée.

## TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION RELATIVE  
A LA PRESENTATION OU A LA TRANSMISSION  
DU DOCUMENT DE PRIORITE

(instruction administrative 411 du PCT)

Expéditeur : le BUREAU INTERNATIONAL

Destinataire:

DENIS, Hervé  
Bull S.A.  
68, route de Versailles  
P.C. : 58D20  
F-78434 Louveciennes Cedex  
FRANCE

Date d'expédition (jour/mois/année)

30 juillet 2001 (30.07.01)

Référence du dossier du déposant ou du mandataire  
PCT 3897 HD

## NOTIFICATION IMPORTANTE

Demande internationale no  
PCT/FR01/01564

Date du dépôt international (jour/mois/année)

22 mai 2001 (22.05.01)

Date de publication internationale (jour/mois/année)  
Pas encore publiée

Date de priorité (jour/mois/année)

25 mai 2000 (25.05.00)

Déposant:

HABERT, Michel

- La date de réception (sauf lorsque les lettres "NR" figurent dans la colonne de droite) par le Bureau international du ou des documents de priorité correspondant à la ou aux demandes énumérées ci-après est notifiée au déposant. Sauf indication contraire consistant en un astérisque figurant à côté d'une date de réception, ou les lettres "NR", dans la colonne de droite, le document de priorité en question a été présenté ou transmis au Bureau international d'une manière conforme à la règle 17.1.a) ou b).
- Ce formulaire met à jour et remplace toute notification relative à la présentation ou à la transmission du document de priorité qui a été envoyée précédemment.
- Un astérisque(\*) figurant à côté d'une date de réception dans la colonne de droite signale un document de priorité présenté ou transmis au Bureau international mais de manière non conforme à la règle 17.1.a) ou b). Dans ce cas, l'attention du déposant est appelée sur la règle 17.1.c) qui stipule qu'aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.
- Les lettres "NR" figurant dans la colonne de droite signalent un document de priorité que le Bureau international n'a pas reçu ou que le déposant n'a pas demandé à l'office récepteur de préparer et de transmettre au Bureau international, conformément à la règle 17.1.a) ou b), respectivement. Dans ce cas, l'attention du déposant est appelée sur la règle 17.1.c) qui stipule qu'aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Date de prioritéDemande de priorité n°Pays, office régional ou  
office récepteur selon le PCTDate de réception du  
document de priorité

25 mai 2000 (25.05.00) 00/06693

FR

13 juil 2001 (13.07.01)

Bureau international de l'OMPI  
34, chemin des Colombettes  
1211 Genève 20, Suisse

Fonctionnaire autorisé:

Fiona DOHERTY

no de télécopieur (41-22) 740.14.35

no de téléphone (41-22) 338.83.38

## REQUÊTE

Le soussigné requiert que la présente demande internationale soit traitée conformément au Traité de coopération en matière de brevets.

Réservé à l'office récepteur	
PCT/FR 01/01564	
Demande internationale n°	
22 MAI 2001 (22/05/01)	
Date du dépôt international	
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE	
DEMANDE INTERNATIONALE PCT	
Nom de l'office récepteur et "Demande internationale PCT"	
Référence du dossier du déposant ou du mandataire (facultatif) (12 caractères au maximum)	
PCT 3897 HD	

<b>Cadre n° I TITRE DE L'INVENTION</b>	
<b>Procédé et architecture de système de communication sécurisé entre deux entités connectées à un réseau de type internet, comprenant un segment de transmissions sans fil.</b>	

<b>Cadre n° II DÉPOSANT</b>	
<p>Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)</p> <p><b>HABERT Michel</b> 4, impasse J.H. Lartigue 38120 SAINT-EGREVE FRANCE</p>	
<p><input checked="" type="checkbox"/> Cette personne est aussi inventeur.</p> <p><input type="checkbox"/> n° de téléphone</p> <p><input type="checkbox"/> n° de télécopieur</p> <p><input type="checkbox"/> n° de téléimprimeur</p>	

Nationalité (nom de l'Etat) : <b>FRANCE</b>	Domicile (nom de l'Etat) : <b>FRANCE</b>
<p>Cette personne est déposant pour : <input checked="" type="checkbox"/> tous les Etats désignés <input type="checkbox"/> tous les Etats désignés sauf les Etats-Unis d'Amérique <input type="checkbox"/> les Etats-Unis d'Amérique seulement <input type="checkbox"/> les Etats indiqués dans le cadre supplémentaire</p>	

<b>Cadre n° III AUTRE(S) DÉPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)</b>	
<p>Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)</p>	
<p>Cette personne est :</p> <p><input type="checkbox"/> déposant seulement</p> <p><input type="checkbox"/> déposant et inventeur</p> <p><input type="checkbox"/> inventeur seulement (Si cette case est cochée ne pas remplir la suite.)</p>	

Nationalité (nom de l'Etat) :	Domicile (nom de l'Etat) :
<p>Cette personne est déposant pour : <input type="checkbox"/> tous les Etats désignés <input type="checkbox"/> tous les Etats désignés sauf les Etats-Unis d'Amérique <input type="checkbox"/> les Etats-Unis d'Amérique seulement <input type="checkbox"/> les Etats indiqués dans le cadre supplémentaire</p>	

D'autres déposants ou inventeurs sont indiqués sur une feuille annexe.

<b>Cadre n° IV MANDATAIRE OU REPRÉSENTANT COMMUN; OU ADRESSE POUR LA CORRESPONDANCE</b>	
<p>La personne dont l'identité est donnée ci-dessous est/a été désignée pour agir au nom du ou des déposants auprès des autorités internationales compétentes, comme:</p>	
<p>Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays.)</p> <p><b>DENIS Hervé</b> <b>BULL S.A.</b> 68, route de Versailles (P.C. : 58D20) 78434 LOUVECIENNES Cedex France</p>	
<p><input type="checkbox"/> n° de téléphone 33 (1) 39.66.61.80</p> <p><input type="checkbox"/> n° de télécopieur 33 (1) 39.66.61.73</p> <p><input type="checkbox"/> n° de téléimprimeur</p>	
<p><input type="checkbox"/> Adresse pour la correspondance : cocher cette case lorsque aucun mandataire ni représentant commun n'est/n'a été désigné et que l'espace ci-dessus est utilisé pour indiquer une adresse spéciale à laquelle la correspondance doit être envoyée.</p>	

## Cadre n° V DÉSIGNATION D'ÉTATS

Les désignations suivantes sont faites conformément à la règle 4.9.a) (cocher les cases appropriées au moins doit l'être) :

## Brevet régional

AP Brevet ARIPO : GH Ghana, GM Gambie, KE Kenya, LS Lesotho, MW Malawi, MZ Mozambique, SD Soudan, SL Sierra Leone, SZ Swaziland, TZ République-Unie de Tanzanie, UG Ouganda, ZW Zimbabwe et tout autre État qui est un État contractant du Protocole de Harare et du PCT

EA Brevet eurasien : AM Arménie, AZ Azerbaïdjan, BY Bélarus, KG Kirghizistan, KZ Kazakhstan, MD République de Moldova, RU Fédération de Russie, TJ Tadjikistan, TM Turkménistan et tout autre Etat qui est un État contractant de la Convention sur le brevet eurasien et du PCT

EP Brevet européen : AT Autriche, BE Belgique, CH et LI Suisse et Liechtenstein, CY Chypre, DE Allemagne, DK Danemark, ES Espagne, FI Finlande, FR France, GB Royaume-Uni, GR Grèce, IE Irlande, IT Italie, LU Luxembourg, MC Monaco, NL Pays-Bas, PT Portugal, SE Suède et tout autre État qui est un État contractant de la Convention sur le brevet européen et du PCT

OA Brevet OAPI : BF Burkina Faso, BJ Bénin, CF République centrafricaine, CG Congo, CI Côte d'Ivoire, CM Cameroun, GA Gabon, GN Guinée, GW Guinée-Bissau, ML Mali, MR Mauritanie, NE Niger, SN Sénégal, TD Tchad, TG Togo et tout autre État qui est un État membre de l'OAPI et un État contractant du PCT (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée)

## Brevet national (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée) :

<input type="checkbox"/> AE Émirats arabes unis	<input type="checkbox"/> LC Sainte-Lucie	
<input type="checkbox"/> AG Antigua-et-Barbuda	<input type="checkbox"/> LK Sri Lanka	
<input type="checkbox"/> AL Albanie	<input type="checkbox"/> LR Liberia	
<input type="checkbox"/> AM Arménie	<input type="checkbox"/> LS Lesotho	
<input type="checkbox"/> AT Autriche	<input type="checkbox"/> LT Lituanie	
<input type="checkbox"/> AU Australie	<input type="checkbox"/> LU Luxembourg	
<input type="checkbox"/> AZ Azerbaïdjan	<input type="checkbox"/> LV Lettonie	
<input type="checkbox"/> BA Bosnie-Herzégovine	<input type="checkbox"/> MA Maroc	
<input type="checkbox"/> BB Barbade	<input type="checkbox"/> MD République de Moldova	
<input type="checkbox"/> BG Bulgarie	<input type="checkbox"/> MG Madagascar	
<input type="checkbox"/> BR Brésil	<input type="checkbox"/> MK Ex-République yougoslave de Macédoine	
<input type="checkbox"/> BY Bélarus	<input type="checkbox"/> MN Mongolie	
<input type="checkbox"/> BZ Belize	<input type="checkbox"/> MW Malawi	
<input type="checkbox"/> CA Canada	<input type="checkbox"/> MX Mexique	
<input type="checkbox"/> CH et LI Suisse et Liechtenstein	<input type="checkbox"/> MZ Mozambique	
<input type="checkbox"/> CN Chine	<input type="checkbox"/> NO Norvège	
<input type="checkbox"/> CR Costa Rica	<input type="checkbox"/> NZ Nouvelle-Zélande	
<input type="checkbox"/> CU Cuba	<input type="checkbox"/> PL Pologne	
<input type="checkbox"/> CZ République tchèque	<input type="checkbox"/> PT Portugal	
<input type="checkbox"/> DE Allemagne	<input type="checkbox"/> RO Roumanie	
<input type="checkbox"/> DK Danemark	<input type="checkbox"/> RU Fédération de Russie	
<input type="checkbox"/> DM Dominique	<input type="checkbox"/> SD Soudan	
<input type="checkbox"/> DZ Algérie	<input type="checkbox"/> SE Suède	
<input type="checkbox"/> EE Estonie	<input type="checkbox"/> SG Singapour	
<input type="checkbox"/> ES Espagne	<input type="checkbox"/> SI Slovénie	
<input type="checkbox"/> FI Finlande	<input type="checkbox"/> SK Slovaquie	
<input type="checkbox"/> GB Royaume-Uni	<input type="checkbox"/> SL Sierra Leone	
<input type="checkbox"/> GD Grenade	<input type="checkbox"/> TJ Tadjikistan	
<input type="checkbox"/> GE Géorgie	<input type="checkbox"/> TM Turkménistan	
<input type="checkbox"/> GH Ghana	<input type="checkbox"/> TR Turquie	
<input type="checkbox"/> GM Gambie	<input type="checkbox"/> TT Trinité-et-Tobago	
<input type="checkbox"/> HR Croatie	<input type="checkbox"/> TZ République-Unie de Tanzanie	
<input type="checkbox"/> HU Hongrie	<input type="checkbox"/> UA Ukraine	
<input type="checkbox"/> ID Indonésie	<input type="checkbox"/> UG Ouganda	
<input type="checkbox"/> IL Israël	<input checked="" type="checkbox"/> US États-Unis d'Amérique	
<input type="checkbox"/> IN Inde	<input type="checkbox"/> UZ Ouzbékistan	
<input type="checkbox"/> IS Islande	<input type="checkbox"/> VN Viet Nam	
<input type="checkbox"/> JP Japon	<input type="checkbox"/> YU Yougoslavie	
<input type="checkbox"/> KE Kenya	<input type="checkbox"/> ZA Afrique du Sud	
<input type="checkbox"/> KG Kirghizistan	<input type="checkbox"/> ZW Zimbabwe	
<input type="checkbox"/> KP République populaire démocratique de Corée	Case réservée pour la désignation d'États qui sont devenus parties au PCT après la publication de la présente feuille :	
<input type="checkbox"/> KR République de Corée	<input type="checkbox"/>	
<input type="checkbox"/> KZ Kazakhstan	<input type="checkbox"/>	

Déclaration concernant les désignations de précaution : outre les désignations faites ci-dessus, le déposant fait aussi conformément à la règle 4.9.b) toutes les désignations qui seraient autorisées en vertu du PCT, à l'exception de toute désignation indiquée dans le cadre supplémentaire comme étant exclue de la portée de cette déclaration. Le déposant déclare que ces désignations additionnelles sont faites sous réserve de confirmation et que toute désignation qui n'est pas confirmée avant l'expiration d'un délai de 15 mois à compter de la date de priorité doit être considérée comme retirée par le déposant à l'expiration de ce délai. (La confirmation (y compris les taxes) doit parvenir à l'office récepteur dans le délai de 15 mois.)

## Cadre n° VI REVENDICATION DE PRIORITÉ

D'autres revendications de priorité sont énoncées dans le cadre supplémentaire.

Date de dépôt de la demande antérieure (jour/mois/année)	Numéro de la demande antérieure	Lorsque la demande antérieure est une :		
		demande nationale : pays	demande régionale :* office régional	demande internationale : office récepteur
(1) 25 mai 2000 (25.05.2000)	0006693	FRANCE		
(2)				
(3)				

L'office récepteur est prié de préparer et de transmettre au Bureau international une copie certifiée conforme de la ou des demandes antérieures (seulement si la demande antérieure a été déposée auprès de l'office qui, aux fins de la présente demande internationale, est l'office récepteur) indiquées ci-dessus au(x) point(s) : 1

\* Si la demande antérieure est une demande ARIPO, il est obligatoire d'indiquer dans le cadre supplémentaire au moins un pays partie à la Convention de Paris pour la protection de la propriété industrielle pour lequel cette demande antérieure a été déposée (règle 4.10.b)ii)). Voir le cadre supplémentaire.

## Cadre n° VII ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Choix de l'administration chargée de la recherche internationale (ISA) (si plusieurs administrations chargées de la recherche internationale sont compétentes pour procéder à la recherche internationale, indiquer l'administration choisie; le code à deux lettres peut être utilisé) :	Demande d'utilisation des résultats d'une recherche antérieure; mention de cette recherche (si une recherche antérieure a été effectuée par l'administration chargée de la recherche internationale ou demandée à cette dernière) :
ISA / FRANCE	Date (jour/mois/année) Numéro Pays (ou office régional) 25.05.2000 0006693 FRANCE

## Cadre n° VIII BORDEREAU; LANGUE DE DÉPÔT

La présente demande internationale contient le nombre de feuillets suivant :	Le ou les éléments cochés ci-après sont joints à la présente demande internationale :
requête : 3	1. <input type="checkbox"/> feuille de calcul des taxes
description (sauf partie réservée au listage des séquences) : 21	2. <input checked="" type="checkbox"/> pouvoir distinct signé
revendications : 5	3. <input type="checkbox"/> copie du pouvoir général; numéro de référence, le cas échéant :
abrégé : 1	4. <input type="checkbox"/> explication de l'absence d'une signature
dessins : 6	5. <input type="checkbox"/> document(s) de priorité indiqué(s) dans le cadre n° VI au(x) point(s) :
partie de la description réservée au listage des séquences :	6. <input type="checkbox"/> traduction de la demande internationale en (langue) :
Nombre total de feuillets : [35] [36]	7. <input type="checkbox"/> indications séparées concernant des micro-organismes ou autre matériel biologique déposés
	8. <input type="checkbox"/> listage des séquences de nucléotides ou d'acides aminés sous forme déchiffrable par ordinateur
	9. <input checked="" type="checkbox"/> autres éléments (préciser) : Dessin abrégé

Figure des dessins qui doit accompagner l'abrégé : 9 Langue de dépôt de la demande internationale : Français

## Cadre n° IX SIGNATURE DU DÉPOSANT OU DU MANDATAIRE

À côté de chaque signature, indiquer le nom du signataire et, si cela n'apparaît pas clairement à la lecture de la requête, à quel titre l'intéressé signe.

Hervé DENIS (Mandataire Bull S.A.)

Réservé à l'office récepteur	
1. Date effective de réception des pièces supposées constituer la demande internationale :	22 MAI 2001 (22/05/01)
3. Date effective de réception, rectifiée en raison de la réception ultérieure, mais dans les délais, de documents ou de dessins complétant ce qui est supposé constituer la demande internationale :	
4. Date de réception, dans les délais, des corrections demandées selon l'article 11.2) du PCT :	
5. Administration chargée de la recherche internationale (si plusieurs sont compétentes) : ISA /	6. <input type="checkbox"/> Transmission de la copie de recherche différée jusqu'au paiement de la taxe de recherche.

Réservé au Bureau international	
Date de réception de l'exemplaire original par le Bureau international : 13 JUILLET 2001	(13.07.01)

**Procédé et architecture de système de communication sécurisé entre deux entités connectées à un réseau de type Internet comprenant un segment de transmissions sans fil**

5 L'invention concerne un procédé de communication sécurisé entre deux entités connectées à un réseau de type Internet.

Elle s'applique plus particulièrement à des communications via un réseau de type Internet comprenant un segment de transmissions sans fil.

10 L'invention concerne encore une architecture de système de communication pour la mise en œuvre de ce procédé.

15 Dans le cadre de l'invention, le terme "entité" doit être entendu dans son sens le plus général. Il s'agit aussi bien de ressources informatiques, matérielles ou logicielles, que, selon une caractéristique de l'invention qui sera explicitée ci-après, d'êtres humains, utilisateurs d'un des composants du système de communication.

20 Le terme "Internet" doit également être compris dans son sens le plus général. Il englobe, outre le réseau Internet proprement dit, les réseaux privés d'entreprises ou similaires, du type dit "intranet", et les réseaux les prolongeant vers l'extérieur, du type dit "extranet", de façon générale tout réseau dans lequel les échanges de données s'effectuent selon un protocole du type Internet. Cependant, pour fixer les idées, sans que cela limite en quoi que ce soit la portée de l'invention, on se placera ci-après dans le cas du réseau Internet proprement dit, sauf mention contraire.

25 Habituellement, les communications sur les réseaux, quelle qu'en soit la nature, s'effectuent conformément à des protocoles répondant à des standards comprenant plusieurs couches logicielles superposées.

30 L'architecture des réseaux de communication est décrite par diverses couches logiques. A titre d'exemple, le standard "OSI" ("Open System Interconnection"), défini par l' "ISO", comporte sept couches qui vont des couches dites basses (par exemple la couche dite "physique" qui concerne le support de transmission physique) aux couches dites hautes (par exemple la couche dite d' "application"), en passant par des couches intermédiaires,

notamment la couche dite de "transport". Une couche donnée offre ses services à la couche qui lui est immédiatement supérieure et requiert de la couche qui lui immédiatement inférieure d'autres services, via des interfaces appropriées. Les couches communiquent à l'aide de primitives. Elles peuvent également 5 communiquer avec des couches de même niveau. Dans certaines architectures, l'une ou l'autre de ces couches peuvent être inexistantes.

Dans le cas d'un réseau de type Internet, les communications s'effectuent selon des protocoles, spécifiques à ce type de communications, mais qui comprennent également plusieurs couches logicielles. Les couches 10 sont au nombre de cinq, et de façon plus précise, en allant de la couche supérieure à la couche inférieure : la couche d'application ("http", "ftp", "e-mail", etc.), la couche de transport ("TCP"), la couche d'adressage de réseau ("IP"), la couche de liens de données ("PPP", "Slip", etc.) et la couche physique. Le protocole de communication est choisi en fonction de l'application plus 15 particulièrement visée : interrogation de pages "WEB" ("HTTP"), transferts de fichiers "FTP", courrier électronique (e-mel, ou "e-mail" selon la terminologie anglo-saxonne), forums ou "news", etc.

Dans sa globalité, un réseau de type Internet comprend tout d'abord un ou plusieurs réseaux de transmission de données proprement dits, 20 éventuellement divisés en sous-réseaux. Ces réseaux comprennent notamment des canaux de liaison physique qui constituent le niveau le plus bas. Les communications peuvent être assurées par des liaisons à relativement bas débit : liaisons téléphoniques, ou des liaisons à haut ou très haut débit : fibres optiques, faisceaux hertziens, liaisons satellites, notamment pour les artères 25 principales. A ce ou ces réseau(x) sont connectés de nombreux systèmes, sous-systèmes, machines et/ou terminaux divers. La connexion peut être directe (à l'aide d'un modem, par exemple) ou indirecte, par l'intermédiaire d'un système dit "fire-wall" (ou "pare-feu"), d'un "proxy", ou par l'intermédiaire du système informatique d'un fournisseur d'accès au réseau Internet (ou "ISP" selon la 30 terminologie anglo-saxonne).

La gamme des entités connectées, dans l'art connu, peut aller des ordinateurs très puissants (par exemple du type dit "main-frame") jusqu'à des

terminaux "légers", c'est-à-dire ne possédant que peu de ressources informatiques propres, par exemple des terminaux dédiés, voire de simples terminaux lecteurs de carte à puce. Ces entités, que l'on peut appeler de façon générique "systèmes", disposent d'un système d'exploitation (ou "OS" selon la terminologie anglo-saxonne), d'un type dit propriétaire ou non. A titre d'exemple, on peut citer le système d'exploitation "UNIX" (marque déposée"), très utilisé dans le cadre des applications relatives au réseau Internet.

Généralement, les communications entre entités connectées s'effectuent selon un mode dit client-serveur et mettent en œuvre la technologie dite d'objets.

10 Un serveur peut être défini comme étant un logiciel, une application ou toute entité logicielle rendant un service donné (par exemple le transfert d'un fichier requis). Une telle entité est hébergée par des systèmes connectés au réseau Internet, que l'on appelle "serveurs". Une entité "client" peut être définie comme étant le dual de l'entité "serveur", c'est-à-dire demandant un service déterminé.

15 Cependant, rien ne s'oppose à ce qu'un système ou une application soit à la fois "client" et "serveur".

Comme il a été indiqué, une des couches logicielle de communication est constituée par la couche d'adressage dite "IP". Il est en effet nécessaire qu'un client, par exemple, puisse adresser sélectivement un serveur, via le réseau Internet. Pour ce faire, la technologie Internet met en œuvre le concept dit d' "URL" (pour "Uniform Resource Locator") faisant appel à une adresse appelée "IP" (pour "Internet protocol"). Le réseau Internet est fortement hiérarchisé en domaines et sous-domaines, qui correspondent eux-mêmes à des réseaux et sous-réseaux, gérés par des systèmes d'annuaires électroniques, 20 dénommés "DNS" (pour "Domains Name Servers"). La structure de l'adresse "IP" reflète cette hiérarchisation. Elle comprend une adresse "IP" proprement dite, comprenant elle-même une adresse de sous-réseau appelée et une adresse d'une entité à l'intérieur de ce sous-réseau. Elle est associée à un numéro de port permettant d'adresser un serveur à l'intérieur de l'entité précitée.

25

30 Pour une même entité connectée au réseau Internet, les adresses "IP" peuvent être permanentes ou variables dans le temps. A titre d'exemple, les

systèmes connectés au réseau Internet, via un fournisseur d'accès, se voient généralement attribuer une adresse différente au début de chaque session.

Dans une période récente, un certain nombre de besoins se sont fait sentir.

5 Un premier besoin concerne la mobilité. On parle de "nomadisme" des utilisateurs. Ceux-ci disposant de terminaux eux-mêmes mobiles, tels des micro-ordinateurs portables, ils désirent pouvoir se connecter à n'importe quel endroit du réseau, sans contraintes excessives. Notamment, la migration d'un domaine à un autre devrait être transparente pour l'usager. Il doit également pouvoir 10 conserver son environnement habituel, par exemple conserver un accès à une liste de services auxquels il est abonné, gratuitement ou non, à un carnet d'adresses, etc. Les données caractérisant cet environnement peuvent être stockées dans un serveur éloigné auquel l'abonné peut accéder. Il peut encore les transporter avec lui, par exemple dans la mémoire d'une carte à puce.

15 Plus récemment, il a été proposé de connecter directement des téléphones mobiles, seuls ou combinés avec des appareils du type organisateur ou similaire, au réseau Internet. Cette connexion s'effectue physiquement par l'intermédiaire d'un réseau de transmissions sans fil, tel le réseau à la norme "Global System for Mobile communications (acronyme de "GSM"). Ce réseau est 20 lui-même connecté au réseau Internet par l'intermédiaire de passerelles spécialisées ou "gateway" selon la dénomination anglo-saxonne.

Cette disposition est très avantageuse, car elle autorise une mobilité extrême. Il n'est plus nécessaire de disposer de points fixes pour se connecter au réseau Internet. *A priori*, la seule limite à cette mobilité résulte de la 25 couverture territoriale, plus ou moins étendue, du réseau "GSM" d'un opérateur donné.

Cependant, il existe d'autres types de limitations dues à ce mode de transmission.

Une première limitation est relative à la bande passante. Dans l'état 30 actuel des technologies, la vitesse de transmission est très faible : 9600 bits/s. Même dans le cas d'une simple ligne téléphonique filaire classique, la norme V90, par exemple, permet d'atteindre une vitesse maximale de

56000 bits/s. On peut obtenir des vitesses bien plus élevées si on fait appel à la technologie "ADSL" (470 kits/s à 1 Mbits/s). En outre, les liaisons de type "RNIS", par câble ou satellites permettent de hauts ou très hauts débits. De nouvelles technologies sont en cours d'étude ou d'implantation, telle "GPRS" 5 ("Global Packet Radio Service") ou "UTMS" ("Universal Mobile Telecommunication Service") et autoriseront de plus grandes vitesses de transmission, mais ne sont pas encore toutes opérationnelles. Pour le moins, le réseau "GSM", dans sa version actuelle, subsistera pendant un laps de temps indéterminé, car des modifications et/ou des changements complets de 10 matériels s'avéreront nécessaires, ce sera le cas notamment pour la version dite "G3" de "GSM".

Une deuxième limitation, corollaire de la miniaturisation des dispositifs de communication sans fil, tient à la surface réduite, voire très réduite des écrans de visualisation de ces dispositifs.

15 Il s'ensuit que les protocoles Internet, notamment en ce qui concerne le "WEB" proprement dit (protocole "HTTP") ne sont pas adaptés. En particulier, le langage couramment utilisé pour ces applications est un langage interprété de description de pages, dit "HTML" ("HyperText Markup Language"), ce langage ne convient pas aux types d'écrans précités.

20 Aussi, il a été proposé un nouveau protocole, dérivé des protocoles de type Internet, de type propriétaire, appelé "WAP" pour "Wireless Application Protocol". Ce protocole permet, à des téléphones mobiles d'accéder à des applications de type "e-mail", "WEB" ou multimédia (vidéo par exemple), en tenant compte des caractéristiques spécifiques de ces appareils et du réseau de 25 communication auquel ils sont connectés (par exemple le réseau "GSM").

Même si elle permet l'accès aux applications ci-dessus, cette solution n'est pas sans inconvénients.

30 Les sites Internet doivent être adaptés, car il n'est pas possible d'afficher sur l'écran d'un téléphone mobile, de surplus habituellement monochrome, ce qui est affichable sur un écran de plus grandes dimensions et définition, tel celui d'un micro-ordinateur. Un langage spécifique a été élaboré

pour ces usages : le "WML" ("WAP Markup Language"). Il est alors nécessaire de disposer d'un navigateur spécifique.

La plupart des services proposés par les opérateurs de téléphonie ayant recours à la technologie "WAP" concernent des services du type accès aux cotations de bourse, aux prévisions météorologiques, à des horaires de trains ou autres moyens de transport, aux horaires de spectacles divers, etc., ou à l'affichage de vidéogrammes simples ou à des jeux peu gourmands en ressources informatiques.

10 Cependant, le recours à cette solution, pour des applications de type commerce électronique ou de type bancaire, par exemple, pose des problèmes relatifs à la sécurité, comme il va l'être montré ci-après.

En effet, un autre besoin qui se fait sentir, dans de nombreux domaines d'application est le niveau de sécurité offert par le système lors des transmissions entre deux entités.

15 Dans le cadre de l'invention, le terme "sécurité" doit être entendu dans un sens général. Il concerne tout d'abord la confidentialité : certaines données sont dites sensibles et ne doivent pas pouvoir être accessibles, à des entités non autorisées, personnes physiques ou applications logicielles. Pour ce faire, on a recours habituellement à diverses techniques de chiffrage. La sécurité 20 concerne aussi les problèmes d'authentification entre parties, d'autant plus aigus que ces parties peuvent être mobiles sur le réseau Internet. L'authentification peut s'effectuer à l'aide de données d'identification (mots de passe) et/ou en ayant recours à la technique dite de certificats, en association avec des clés de chiffrage, par exemple stockées dans une carte à puce. La sécurité concerne 25 aussi ce qui relève de l'intégrité des données transmises. On doit pouvoir s'assurer que les données reçues n'ont pas subi de modifications non désirées, que ce soit de manière accidentelle (défaillance des circuits de transmission par exemple) ou intentionnelles (malveillance, etc.). Pour ce faire, on peut mettre en œuvre des techniques de redondance et/ou des techniques de signature 30 électronique (scellement).

Pour le réseau Internet "classique", une des techniques de sécurisation les plus utilisées fait appel à la technologie dite "SSL/TLS" ("secure Socket

Layer/Transport Layer Security"). Cependant cette technologie n'assure qu'un niveau de sécurité minimal. Un niveau supérieur, d'ailleurs rendu obligatoire par la version dite "IPV6" des protocoles Internet (c'est-à-dire la version 6, la version actuellement utilisée étant majoritairement la version 4 ou "IPV4"), est assuré par le protocole de sécurité connu sous le sigle "IPSec". Il s'agit d'un niveau de sécurité standardisée permettant une sécurisation de bout en bout, au niveau réseau.

Dans le cas de la technologie "WAP", il a été proposé une couche de sécurité ayant une fonctionnalité analogue à la couche "SSL/TLS" précitée, utilisable pour les transmissions sans fil et connue sous le sigle "WTLS" ("Wireless Transport Layer Security"). Cette technologie, d'usage optionnel, introduit un niveau de complexité important et n'offre pas un niveau de sécurité élevé. Aussi, puisque comme il a été rappelé, la majorité des services offerts ne nécessitant pas de mesures de sécurité particulières, les opérateurs des réseaux téléphoniques sont peu enclin à la mettre en œuvre.

En outre, et surtout, comme il a été indiqué, il existe en général une passerelle, ou "gateway", assurant l'interface entre le réseau Internet et le réseau de transmissions sans fil.

La figure 1, placée en fin de la présente description, illustre schématiquement une architecture, selon l'art connu, d'un système de communication 1 entre un utilisateur  $U_1$ , muni d'un terminal mobile de type "WAP" 10 (par exemple un téléphone mobile"), connecté à un réseau de radio-transmission  $RTT$  (par exemple au standard "GSM" ou "GPRS"), et un dispositif informatique 12, connecté au réseau Internet  $RI$ , par exemple un serveur éloigné. Le terminal mobile 10 à un rôle de client vis-à-vis du serveur 12. Le réseau  $RTT$  forme le segment "aérien" du réseau de communication mobile, segment relié à un second segment  $RT$ , appelé réseau public terrestre mobile, ou sous le sigle anglo-saxon "PLMN" ("Public Land Mobile Networks"), via des balises émettrices/réceptrices (non représentées) définissant des cellules.

Cette technologie est bien connue de l'homme de métier et ne nécessite pas d'être décrite plus avant. On pourra se référer avec profit, à titre d'exemple non limitatif, à l'article de Jean CELLMER, intitulé "Réseaux

cellulaires, Système GSM", paru dans les "Techniques de l'Ingénieur", Volume TE 7364, novembre 1999, pages 1 à 23.

Le réseau Internet *RI* est interconnecté au segment *RT*.

Les segments terrestres *RT* et aériens *RTT* sont interconnectés par 5 une passerelle 11. Dans le cadre de la technologie "WAP", cette passerelle 11 joue également un rôle d'interface assurant des conversions bilatérales "WAP" de ou vers "HTTP". Elle comprend notamment une couche logique de protocole "WAP" 110a et une couche logique de protocole "HTTP" 111a, complétée par une couche de sécurité "SSL/TLS" 111b, du côté "HTTP", et une couche 10 (optionnelle) de sécurité "WTLS" 110b, du côté "WAP".

La passerelle 11 comprend enfin une interface 113 entre les deux séries de couches logiques destinées à effectuer la conversion bilatérale précitée. Or, précisément, cette interface 113, entre les protocoles de sécurité, "SSL/TLS" 111b et "WTLS" 110b introduit une faille de sécurité, ce qui crée une zone 15 d'insécurité qui rend le concept dit "WAP gateway" qui vient d'être décrit incompatible, de façon pratique, avec le commerce électronique, les applications bancaires, et de façon plus générale avec toute application dite sensible exigeant un niveau de sécurité élevé.

Par contre, si l'on considère une station de travail 13, ou tout dispositif 20 similaire sous le contrôle d'un usager  $U_2$ , connectée directement au réseau Internet *RI*, les protocoles de communication utilisés entre cette station de travail 13 et le serveur 12 restent homogènes. Il n'existe pas de faille de sécurité intrinsèque au système. Il en aurait été de même, si la station de travail 13 avait été connectée au serveur 12 via un réseau intranet ou extranet.

25 L'invention vise à remplir les besoins qui se font sentir pour les communications via un réseau de type Internet, que ce soit un réseau de type classique ou un réseau mettant en œuvre la technologie "WAP", tout en palliant les inconvénients des dispositifs de l'art connu, et dont certains viennent d'être rappelés.

30 Pour ce faire, selon une première caractéristique, le concept précité dit "WAP gateway" est entièrement éliminé, ce qui permet de supprimer la faille de

sécurité constatée au niveau de l'interface "WEB/WAP". La conversion "WAP/WEB" est effectuée directement au niveau des serveurs.

Selon une deuxième caractéristique, on attribue à chacune des entités devant être mise en relation une adresse dite permanente.

5 Selon une autre caractéristique, on adopte un mécanisme de sécurité de bout en bout, au niveau réseau, utilisable pour toute application de type Internet, "WEB", "WAP", ou autre, et qui est programmé de manière déclarative ce qui assure une transparence complète.

10 Du fait de cette transparence, une des conséquences avantageuses du procédé selon l'invention est qu'il n'est pas nécessaire de réécrire les applications existantes pour les sécuriser avec cette technique.

Dans une variante préférée de réalisation de l'invention, le mécanisme adopté est le protocole "IPSec" précité.

15 Bien que le procédé selon l'invention soit particulièrement avantageux lorsqu'un des segments du réseau de communication est constitué par un réseau de communication sans fil impliquant l'utilisation de la technologie "WAP", il doit être clair qu'il s'applique également à un réseau de type Internet homogène.

20 L'invention a donc pour objet principal un procédé de communication sécurisé entre des première et seconde entités interconnectées via un réseau de type Internet, lesdites entités étant associées à des premier et second systèmes de traitement informatique de données parmi un ensemble de systèmes distribués connectés au dit réseau de type Internet, caractérisé en ce que lesdites première et seconde entités sont constituées par une pièce de 25 logicielle hébergée dans un desdits systèmes connectés audit réseau de type Internet et/ou un utilisateur desdits systèmes connectés, en ce que ledit premier système fonctionne en mode dit client et ledit second système fonctionne en mode dit serveur, en ce qu'il comprend une étape d'attribution, sur ledit ensemble de systèmes, d'une adresse permanente de type Internet, du type dit "IP", à chacune desdites entités interconnectées, en ce qu'il est implanté dans ledit second système formant serveur au moins une pièce de logiciel formant serveur et offrant les services d'au moins une application à ladite première 30

entité, et en ce qu'il est implanté dans lesdits premier et second systèmes une pile protocolaire de communication comportant au moins une couche pour l'exécution d'une étape de chiffrement, en mode bout en bout, conforme à un protocole de sécurisation déterminé, de données échangées entre lesdites 5 entités interconnectées.

L'invention a encore pour objet une architecture de communication dans un ensemble de systèmes distribués pour la mise en œuvre du procédé.

L'invention va maintenant être décrite de façon plus détaillée en se référant aux dessins annexés, parmi lesquels :

- la figure 1 illustre schématiquement un exemple de réalisation d'un système de communication, selon l'art connu, comprenant un réseau Internet et un réseau de communication sans fil mettant en œuvre la technologie "WAP" ;
- la figure 2 illustre schématiquement un exemple d'architecture de système de communication via un réseau Internet et un réseau de communication sans fil mettant en œuvre la technologie "WAP", selon un mode de réalisation préféré de l'invention ;
- les figures 3 et 4 illustrent deux variantes de configuration de système serveurs selon l'invention ;
- les figures 5 et 6 illustrent une architecture de système permettant d'adresser directement une application logicielle hébergée par un système ;
- la figure 7 illustre de façon plus détaillée l'interconnexion de deux entités dans le système de la figure 2 ;
- la figure 8 illustre schématiquement une liaison sécurisée du type dit "tunnel" obtenue par le procédé selon l'invention ; et
- la figure 9 illustre un exemple d'architecture de système de communication sécurisée via un réseau Internet pour une application marchande en technologie dite "WAP".

30 Dans ce qui suit, sans en limiter en quoi que ce soit la portée, on se placera ci-après dans le cadre de l'application préférée de l'invention, sauf mention contraire, c'est-à-dire dans le cas d'un système de communication

hybride comprenant un réseau Internet et, éventuellement, un réseau intranet, ainsi qu'un réseau de communication mobile, comportant un segment aérien, et mettant en œuvre la technologie "WAP".

La figure 2 illustre de façon schématique un exemple d'architecture de système, désormais référencée 2, pour la mise en œuvre du procédé conforme à l'invention. Les éléments communs aux figures précédentes portent les mêmes références et ne seront re-décris qu'en tant que de besoin.

Le système 2 de l'exemple de la figure 2, considéré dans sa globalité, comprend tout d'abord un terminal mobile 20, sous le contrôle d'un utilisateur  $U'_1$  (jouant un rôle analogue au terminal 10 de la figure 1), et une station mobile 25, sous le contrôle d'un utilisateur  $U'_3$ , toutes deux connectées au réseau de radio-transmission  $RTT$ . Le terminal 20, supposé être un téléphone mobile, est connecté directement au réseau  $RTT$ . La station mobile 25, par exemple un micro-ordinateur, est connectée à ce réseau  $RTT$  via un équipement terminal 26, qui peut être constitué également par un téléphone mobile. Ce dernier est connecté à la station mobile 25 via une liaison série ou une liaison infrarouge, par exemple.

Comme précédemment, le réseau  $RTT$  est connecté au réseau terrestre  $RT$  par l'intermédiaire d'une passerelle 21. Cependant, cette dernière ne joue plus le rôle d'interface de conversion "WAP – HTTP" (fonction "WAP gateway" précitée), selon un des aspects de l'invention. Elle permet de réaliser, de façon classique en soi, des conversions électriques et logiques nécessaires pour passer d'un mode transmission de données par voie terrestre à un mode de transmission par voie hertzienne, par exemple à la norme "GSM".

Le réseau terrestre  $RT$  est connecté au réseau Internet  $RI$ , ce dernier étant, dans l'exemple de la figure 2, connecté lui-même à un réseau intranet  $it$ , via un serveur d'accès 22. Un serveur 3 est connecté au réseau intranet  $it$ .

On a également représenté une station de travail 24 connectée au réseau intranet  $it$ , par exemple un micro-ordinateur, sous le contrôle d'un utilisateur  $U'_4$ , ainsi qu'une deuxième station de travail 27 connectée directement au réseau Internet  $RI$ , par exemple un micro-ordinateur, sous le contrôle d'un utilisateur  $U'_2$  (jouant un rôle analogue à la station 13 de la figure 1).

Dans la réalité, un nombre beaucoup plus importants d'utilisateurs est connecté aux réseaux du système 2, via divers types de machines ou systèmes. Cependant, le système 2 de la figure 2 permet d'illustrer les principaux types de dispositifs rencontrés sur des réseaux où cohabitent les protocoles Internet standards et "WAP". On peut aussi prévoir des systèmes dits "firewall" ou "pare-feu" (non représentés), par exemple inclus dans le serveur d'accès 22, isolant le réseau intranet *it* du monde extérieur, c'est-à-dire du réseau Internet *Ri*.

Selon une caractéristique, également commune en soi à l'art connu, tout ou partie des machines ou systèmes connectés peut être mobile sur le réseau. Les autres utilisateurs devraient pouvoir adresser de façon transparente les machines qui ont migré. Aussi, au moins dans la version "IPV6" précitée, on prévoit un dispositif 23, connu généralement sous la dénomination anglo-saxonne "Home agent", ici connecté au réseau intranet *it*, permettant de gérer cette mobilité. Pour ce faire, un protocole dit "Mobile IP" est utilisé. Il permet de corréler une adresse temporaire attribuée à un système connecté avec une adresse permanente attribuée à l'entité qui lui est associée. Un utilisateur désirant adresser le système mobile ne manipule toujours que cette seule adresse permanente. Le protocole "Mobile IP" précité permet d'organiser une macro-mobilité. C'est le cas, par exemple, lorsque l'on change d'opérateur de réseau "GPRS".

Cet ensemble constitue un système distribué.

Jusqu'à présent, à l'exception de la structure de la passerelle 21, qui ne sert plus d'interface entre les protocoles "WAP/HTTP", l'architecture générale du système 2 qui vient d'être décrite est commune, en soi, à une architecture selon l'art connu (telle celle de la figure 1).

Selon une première caractéristique propre à l'invention, qui va être décrite en regard des figures 3 et 4, l'architecture des serveurs 3 est modifiée, de façon à ce que des conversions aux protocoles d'interfaces applicatives des serveurs "WEB" soient réalisées à l'intérieur de ceux-ci, et non plus au niveau de la passerelle 21, sous la forme de conversion de protocole de communication "WAP/HTTP". Le serveur 3 héberge donc une passerelle "WAP" avec un adaptateur d'interface applicative de serveur "WEB". Cette modification va

permettre une sécurisation des transmissions, de bout en bout, transparente vis-à-vis des protocoles utilisés, "HHTP", "WAP" ou autres (transmissions en mode paquet de données), ne présentant plus de faille de sécurité comme dans l'art connu, par la disparition de la fonction "WAP gateway". Elle permet enfin de ne 5 plus utiliser le protocole de sécurité "WTLS", complexe à mettre en œuvre et n'offrant qu'un faible niveau de sécurité.

Sur la figure 3, on a supposé que le serveur 3 comprenait à la fois des applications "WAP", sous les références 36a et 36b, et des applications "WEB", sous les références 37a et 37b. Selon un des aspects de l'invention, on prévoit 10 aussi, implantés dans le serveur 3, un serveur dédié "WAP" 30 et un serveur dédié "WEB" 31. Ces deux serveurs, 30 et 31, sont aptes à reconnaître sélectivement les requêtes selon le protocole "WAP" de celles selon le protocole "WEB", respectivement. Cette sélection s'effectue via les configurations particulières des messages reçus appartenant à l'un ou l'autre des protocoles. 15 Les requêtes sont reçues du réseau Internet *RI*, directement ou indirectement par un réseau intranet *it* (figure 2), via des organes classiques (non représentés) : modem, etc., et des couches de communications standardisées (également non représentées).

Selon une première variante de l'invention, illustrée par la figure 3, on 20 interpose un module 32 entre le serveur "WAP" 30 et des "APIs" ou protocoles d'interface applicatives de type serveur "WEB" 33. Ce module 32, pouvant être constitué par une pièce de logiciel, est un adaptateur d'interface permettant que les méthodes d'accès des applications "WAP" soient les mêmes que les méthodes d'accès des applications "WEB" à des serveurs "WEB".

25 Les applications 36a-36b et 37a-37b peuvent être constituées de pages écrites en langages "WLM" et "HTLM", respectivement.

Comme il est bien connu en soi, un certain nombre de techniques sont utilisées pour écrire des applications "WEB" en "dos" de serveur "WEB". Il peut 30 s'agir "d'APIs" de types connus sous les sigles "CGI" (pour "Common Gate Interface", qui constituent une passerelle), "NSAPI" (pour Netscape Server API – marque déposée) ou "ISAPI" (pour Internet Server API). L'application 37b est de ce type et est donc interconnectée directement au module 33. Plus récemment,

on a proposé des "APIs" dits de conteneur (ou "container" selon la terminologie anglo-saxonne) constituant des moteurs dits de "Servlets" (marque déposée). L'application 37a est de ce type et est interconnectée au module 33 via un module connu sous l'appellation "WEB Container" 34 et des "APIs" spécifiques 5 35. A titre d'exemple, on peut citer "TOMCAT", pour des serveurs de type "APACHE", sous système d'exploitation "LINUX" (tous ces termes correspondant à des marques déposées).

10 Selon la caractéristique avantageuse de l'invention qui vient d'être rappelée, le serveur "WAP" 30 dispose donc d'un adaptateur d'interface 32 qui permet aux applications écrites pour des serveurs "WAP" 30 d'utiliser les deux séries de mécanismes standards rappelés ci-dessus : applications "WAP" 36b et 36a respectivement.

15 Une deuxième variante de réalisation de l'invention est illustrée par la figure 4. Le serveur, ici référencé 3', comprend, comme précédemment, un serveur "WAP" 30 et un serveur "WEB" 31, ainsi que le module adaptateur d'interface 32. Cependant les applications présentes dans le serveur 3' sont uniquement des applications de type "WEB", référencées 37a à 37d, *a priori* 20 écrites en langage "HTML". Les applications "WEB" 37a et 37b correspondent aux applications "WEB" de mêmes références sur la figure 3, les applications 37c et 37d se substituant aux applications "WAP" 36a et 36b, respectivement. Des modules supplémentaires 38a et 38b sont intercalés entre les modules 33 et 34-35, d'une part, et les applications 38a et 38b, d'autre part. La fonction 25 dévolue à ces module 38a et 38b est une conversion bidirectionnelle entre les langages "HTML" et "WML". De ce fait, les requêtes en provenance du serveur "WAP" 30 sont transmises via les modules 33 ou 34-35 aux convertisseurs 38a ou 38b, puis à une des applications "WEB" 37c ou 37d. Par contre, les requêtes en provenance du serveur "WEB" 31 sont transmises directement, des modules 33 ou 34-35 aux applications "WEB" 37a ou 37b. Le cheminement inverse est également vrai.

30 Selon une autre caractéristique du procédé de l'invention, une adresse permanente est attribuée aux utilisateurs ou à des applications clientes (par exemple  $U_1$  à  $U_4$ , figure 2), et aux applications serveurs (par exemple 36a-36b

et/ou 37a-37b, figures 3 ou 4). De façon générale, on attribue une adresse permanente aux entités devant être connectées. Cette attribution peut être effectuée de façon dynamique.

5 Dans les réseaux de type Internet actuels, il n'est pas possible d'adresser directement une application à l'intérieur d'un système. En général, des clients qui adressent une entité distante gérée par un système, service ou application, invoquent un service de noms. Celui-ci requiert le nom du réseau et l'adresse du système qui contient l'entité à atteindre.

10 Aussi, la Demanderesse a proposé, dans la demande de brevet français publiée sous le numéro FR 2 773 428 A1, un procédé permettant notamment d'adresser directement une application logicielle hébergée par un système connecté à un réseau de type Internet. Ce procédé va être rappelé brièvement ci-après par référence aux figures 5 et 6.

15 Cette figure 5 illustre schématiquement le procédé d'adressage de serveurs selon cette demande de brevet. Pour simplifier, il a été supposé que l'ensemble des systèmes, référencé 2', était compris dans un domaine  $D$ , unique, associé à un serveur de noms de domaine  $DNS_1$ . On a représenté, également dans un but de simplification, un seul client,  $Cl_1$ . Il peut s'agir, par exemple, de la station de travail 27 de la figure 2. Selon une des caractéristiques 20 du procédé d'adressage, chaque système réel (par exemple les serveurs 3 ou 3' des figures 3 et 4) est assimilé à un réseau virtuel, référencés  $SVN$ , à  $SVN_n$ , représentés en traits pointillés sur la figure 5, appelés arbitrairement "réseaux virtuels systèmes".

25 Selon une deuxième caractéristique du procédé d'adressage, les serveurs, par exemple  $SV_{11}$  à  $SV_{13}$  dans le réseau virtuel système  $SVN_1$ , sont associés chacun à une adresse "IP" individuelle. Il s'ensuit que chaque serveur, par exemple le serveur  $SV_{11}$ , c'est-à-dire un objet ou une entité logicielle, est directement adressable par un client, par exemple le client  $Cl_1$ , et, de façon plus générale, un client  $Cl_x$ , si le système 2' comporte plusieurs clients (x étant arbitraire). En d'autres termes, un client n'a plus besoin de connaître le nom du système hébergeant le serveur recherché. L'annuaire du serveur  $DNS_1$  stocke

toutes les adresses "IP" des serveurs, par exemple des serveurs  $SV_{11}$  à  $SV_{13}$  du réseau virtuel système  $SVN_1$ .

Il doit être noté que, dans un système multidomaines, tous les serveurs d'un réseau virtuel système appartiennent à un même domaine.

5 Selon une troisième caractéristique du procédé d'adressage, les systèmes "réels" ou machines qui constituent, dans une configuration classique, des systèmes terminaux deviennent des systèmes intermédiaires. Ils constituent des nœuds des réseaux virtuels,  $SVN_1$  à  $SVN_n$ , et également des nœuds du réseau "réel", c'est-à-dire le sous-réseau Internet ou intranet  $SR_x$ . Les systèmes 10 agissent en tant que passerelles qui interconnectent les nœuds des réseaux virtuels,  $SVN_1$  à  $SVN_n$ , au sous-réseau  $SR_x$ . Chaque système est également doté d'une adresse "IP".

On peut donc représenter un réseau virtuel système  $SVN_1$  associé à un système  $S_1$ , de la façon illustrée par la figure 6. On constate qu'un système  $S_1$  15 constitue bien un nœud pour le réseau  $R_x$  et qu'il est associé, vu de ce réseau (c'est-à-dire de l'extérieur), à une première adresse  $IP_1$ , avec  $@/IP_1:X,X_1$ ,  $X$  étant le préfixe attribué au sous-réseau  $SR_x$  et  $X_1$  l'adresse de  $S_1$  dans le sous-réseau  $SR_x$ .

On suppose que le réseau virtuel système  $SVN_y$  est constitué des deux 20 serveurs référencés  $SV_A$  et  $SV_B$  qu'il héberge et du système  $S_1$  proprement dit. Vu du réseau virtuel système  $SVN_1$ , le système  $S_1$  est associé à une seconde adresse :  $IP_2$ , avec  $@/IP_2:Y,Y_1$ ,  $Y$  étant le préfixe attribué au réseau virtuel système  $SVN_y$  et  $Y_1$  l'adresse de  $S_1$  dans le réseau  $SVN_y$ .

De même, les serveurs  $SV_A$  et  $SV_B$  sont associés à deux adresses,  $IP_A$  25 et  $IP_B$ , respectivement, avec  $@/IP_A:Y,Y_A$ , et  $@/IP_B:Y,Y_B$ ,  $Y_A$  et  $Y_B$  étant les adresses de  $SV_A$  et  $SV_B$ , respectivement, dans le réseau  $SVN_y$ .

Pour une description plus détaillée du mécanisme d'adressage, on pourra se référer avec profit à la demande de brevet français précitée, notamment à la figure 4 de cette demande qui illustre de façon détaillée 30 l'architecture d'un système réel permettant l'adressage précité.

Dans le cadre de l'invention, les serveurs  $SV_A$  et  $SV_B$  peuvent être constitués par les serveurs "WAP" 30 et "WEB" 31 de la figure 3, le système réel  $S_1$  étant alors le système serveur 3.

Le procédé d'adressage selon la demande de brevet français précité, 5 comme le procédé selon l'invention restent compatibles avec le protocole Internet le plus couramment utilisé ce jour, c'est-à-dire la version "IPV4". Cependant, une adresse conforme à ce protocole ne comporte que quatre octets, soit  $2^{32}$  adresses théoriques, en réalité beaucoup moins du fait de la structure hiérarchique rappelée ci-dessus. Du fait de la croissance rapide du 10 réseau Internet, des projections sur le futur ont montré que cet espace d'adressage limité conduira rapidement à une pénurie. Or le fait de pouvoir adresser directement des entités internes à un système et, selon une des caractéristiques de l'invention, de leur attribuer des adresses permanentes, multiplie les besoins en nombres d'adresses distinctes. Aussi, dans le cadre de 15 l'invention, on préférera le protocole "IPV6" pour l'attribution des adresses permanentes. L'espace d'adressage théorique est alors fortement augmenté : environ  $6,65 \times 10^{23}$  adresses réseau par mètre carré de la surface de la terre.

Comme il a été indiqué, selon une autre caractéristique de l'invention, la 20 sécurisation des transmissions est réalisée de bout en bout, de façon transparente par vis-à-vis des différents protocoles : "WAP", "WEB" ou autres. Dans un mode de réalisation préféré, on adopte le protocole connu sous le sigle "IPSec", protocole d'ailleurs obligatoire si la version "IPV6" est mise en œuvre pour les transmissions sur le réseau Internet.

La figure 7 illustre schématiquement un exemple d'architecture de 25 système de transmission 2, selon l'invention, montrant l'interconnexion entre deux entités de type client, référencées 4 et 4', et une entité de type serveur, 3. Les client 4 ou 4' est constitués par l'un des dispositifs représentés sur la figure 2 : 20, 24, 26 ou 27. Les deux entités, 3 et 4 ou 4', communiquent entre elles par l'intermédiaire d'un ou plusieurs des réseaux de la figure 2, sous la référence 30 unique  $R$ . L'entité 4 est un client de type "WEB" et l'entité 4' un client de type "WAP".

On a supposé que le protocole "IPV4" était utilisé pour les transmissions, ce qui est généralement le cas à l'heure actuelle. Le procédé d'adressage illustré par référence avec les figures 5 et 6, et le procédé selon l'invention sont compatibles avec des réseaux de type, comme il a été rappelé.

5 Dans le cadre de l'invention, on met en œuvre un protocole dénommé "6-to-4" qui convertit les adresses "IPV6" en adresses "IPV4" compatibles "IPV6", et inversement.

Selon le procédé de l'invention on implémente dans chaque système physique une pile protocolaire de communication comprenant successivement

10 une pile "IPV6", 390 ou 44, incluant le protocole de sécurité "IPSec", 391 ou 45, et une pile "IPV4" 392 ou 46, respectivement pour le serveur 3 et les clients 4 ou 4'. Les piles "IPV4", 392 et 46, sont interfacées avec le réseau *R*. Les piles "IPV6", 390 et 44, sont interfacées avec les serveurs "WAP" 30 et "WEB" 31, côté serveur 3, et avec des clients "WAP" 42 et "WEB" 43, côté client 4.

15 Sur la figure 7, on a également détaillé les couches applicatives du client 4, qui présentent une grande symétrie avec celles du serveur 3. les clients, 42 et 42', peuvent être constitués par des navigateurs. Des associations de sécurité sont définies entre des utilisateurs ou des applications clientes et des applications serveurs. De façon avantageuse, un "triplet" identifie chaque

20 association de sécurité :

- une adresse de destination des paquets de données ;
- un protocole de sécurité, de façon préférentielle le protocole dit "ESP" ("Encapsulating Security Payload" ou protocole d'authentification de données) est utilisé en mode tunnel ; et
- un paramètre index de sécurité ("Security Parameter Index" ou "SPI").

On constate que la sécurisation des transmissions, du fait que le chiffrage et le déchiffrage est réalisé en amont des couches d'adresses "IPV4", dans chaque entité à mettre en relation, on obtient bien la sécurisation

30 transparente désirée, de bout en bout. On ne constate plus de faille de sécurité lors du cheminement des données, même si un segment du réseau est du type à transmissions sans fil.

Le schéma équivalent à l'architecture représentée par la figure 7 est celui illustré par la figure 8. Le canal de transmission peut en effet être représenté symboliquement sous la forme d'un câble blindé ou "tunnel" mettant en liaison deux entités, arbitrairement référencées  $E_1$  et  $E_2$ , auxquelles les 5 adresses permanentes respectives  $@IP_{E1}$  et  $@IP_{E2}$  ont été attribuées. Il s'agit, soit d'adresses "IPV6", soit d'adresses compatibles "IPV6" si le réseau est au protocole ""IPV4".

A titre d'exemple, un "tunnel" sécurisé est établi entre un terminal "WAP", par exemple le téléphone mobile 20 (figure 2) et le serveur 3 10 hébergeant une application "WAP" 33. De façon générale, le "tunnel" transporte des communications "IPV6" de bout en bout entre un utilisateur et une application.

Naturellement, si le réseau  $R$  est au protocole "IPV6" les conversions d'adresses ne sont plus nécessaires et les piles "IPV4", 392 et 46 n'existent pas.

15 Lorsque la station connectée est du type mobile, on fait appel au protocole dit "mobile IPV6". La station mobile est associée à chaque instant à une adresse temporaire qui reste transparente pour les utilisateurs désirant adresser l'entité associée à cette station. Un dialogue est initialisé avec un dispositif du type "home agent" précité (figure 2 : 23). Ce dernier établit une 20 corrélation entre l'adresse permanente attribuée et l'adresse temporaire. Cette disposition permet d'obtenir ce qui a été précédemment appelée une "macro-mobilité".

25 Le dialogue précité est sécurisé. De façon préférentielle, le mécanisme d'authentification propre à "IPSec" est mis en œuvre comme le préconise le protocole "mobile IPV6".

On obtient des communications entre utilisateurs et applications avec mise en œuvre des services suivants de "IPSec", s'ils sont sélectionnés :

- authentification de la source de données, incluant l'authentification de l'utilisateur ;
- intégrité ; et
- confidentialité.

En ce qui concerne plus précisément l'authentification des utilisateurs, celle-ci s'effectue avantageusement par l'intermédiaire de l'adresse permanente qui leur est attribuée. Les utilisateurs sont enregistrés dans un annuaire électronique. A titre d'exemple, l'organisme connu sous le sigle "IETF" ("Internet 5 Engineering Task Force") a proposé un standard d'annuaire, que l'on peut qualifier d' "allégé", connu sous le sigle "LDAP" ("Lightweight Directory Access Protocol"). Un profil d'abonné et des privilèges éventuels sont associés à l'utilisateur. Comme "IPSec" est utilisé, avec le mécanisme "ESP", en mode "tunnel" (figure 8), une authentification de la source d'information (une adresse 10 "IPV6" permanente), en l'occurrence l'identification de l'utilisateur, est présente dans chaque paquet de données et chiffrée. En outre, la source de données est authentifiée et, dans ce cas, représente l'utilisateur. Cette identification est utilisée pour construire un contexte de sécurité utilisé lui-même par l'application ou, mieux, par le contenant de l'application pour effectuer un contrôle d'accès 15 pour des contrôles d'autorisation.

Pour fixer les idées, on va maintenant décrire un exemple d'architecture de système de transmission, mettant en œuvre les dispositions de l'invention, adaptée à une application marchande mobile sécurisée, empruntant un tronçon de réseau de radio-transmission par paquets, par exemple du type "GPRS".

20 La figure 9 illustre schématiquement une telle architecture, référencée 2". Les éléments communs aux figures précédentes portent les mêmes références et ne seront re-décrits qu'en tant que de besoin.

Comme précédemment, le système 2", dans sa globalité comprend des terminaux mobiles, dont un seul, 20 sous le contrôle de l'utilisateur  $U_1$ , a été 25 illustré. Ce terminal mobile 20 est connecté au tronçon de réseau sans fil  $RTT$ , puis via la passerelle 21 au réseau terrestre public  $RT$ , au réseau Internet  $RI$ . Un serveur, par exemple du type 3 de la figure 3, hébergeant au moins une application marchande par exemple l'application 36a, en technologie "WAP", est connecté au réseau Internet via le réseau Intranet  $it$  et le serveur d'accès 22. On 30 a également représenté un terminal "WEB" 24 connecté au réseau intranet  $it$ . Ce terminal est similaire à la station 24 de la figure 2.

On n'a pas représenté les piles protocolaires d'adressage et "IPSec" (voir figure 7) permettant d'attribuer des adresses "IPV6" et d'effectuer les opérations nécessitées par le protocole "IPSec".

5 L'architecture qui vient d'être décrite permet d'établir un lien logique *l/s* entre l'utilisateur *U*, et l'application marchande "WAP" 36a, sécurisé de bout en bout, ce malgré le fait qu'il emprunte un segment de réseau sans fil.

A la lecture de ce qui précède, on constate aisément que l'invention atteint bien les buts qu'elle s'est fixés.

10 Il doit être clair cependant que l'invention n'est pas limitée aux seuls exemples de réalisations explicitement décrits, notamment en relation avec les figures 2 à 9.

15 Les applications de l'invention ne se limitent pas non plus au seul domaine "commerce électronique sécurisé". Elles couvrent également des applications bancaires, médicales, et de façon plus générale toute application mettant en œuvre des communications transitant par un réseau de type Internet, notamment dont un segment au moins est constitué par un réseau de transmissions sans fil.

REVENDICATIONS

1. Procédé de communication sécurisé entre des première et seconde entités interconnectées via un réseau de type Internet, lesdites entités étant associées à des premier et second systèmes de traitement informatique de données parmi un ensemble de systèmes distribués connectés au dit réseau de type Internet, caractérisé en ce que lesdites première et seconde entités sont constituées par une pièce de logicielle (36a-36b, 37a-37b) hébergée dans un desdits systèmes (3, 3') connectés audit réseau de type Internet (*R<sub>1</sub>*, *R*) et/ou un utilisateur (*U<sub>1</sub>*) desdits systèmes connectés (4, 20), en ce que ledit premier système (4, 20) fonctionne en mode dit client et ledit second système (3, 3') fonctionne en mode dit serveur, en ce qu'il comprend une étape d'attribution, sur ledit ensemble de systèmes, d'une adresse permanente de type Internet, du type dit "IP", à chacune desdites entités interconnectées (*U<sub>1</sub>*, 36a-36b, 37a-37d), en ce qu'il est implanté dans ledit second système formant serveur (3, 3') au moins une pièce de logiciel formant serveur (30, 31) et offrant les services d'au moins une application (36a-36b, 37a-37d) à ladite première entité (*U<sub>1</sub>*), et en ce qu'il est implanté dans lesdits premier (4, 20) et second (3, 3') systèmes une pile protocolaire de communication comportant au moins une couche (45, 391) pour l'exécution d'une étape de chiffrement, en mode bout en bout, conforme à un protocole de sécurisation déterminé, de données échangées entre lesdites entités interconnectées (*U<sub>1</sub>*, 36a-36b, 37a-37d).  
5  
10  
15  
20  
25
2. Procédé selon la revendication 1, caractérisé en ce que lesdites adresses permanentes "IP" attribuées aux dites entités interconnectées (*U<sub>1</sub>*, 36a-36b, 37a-37d) sont conformes au protocole d'adressage de type Internet "IPV6".
3. Procédé selon la revendication 2, caractérisé en ce que lesdites communications sur ledit réseau de type Internet (*R<sub>1</sub>*, *R*) s'effectuant selon le protocole d'adressage de type Internet "IPV4", il comprend l'implantation dans

lesdits premier (4, 20) et second (3, 3') systèmes d'une couche protocolaire (46, 392) permettant de dériver des adresses "IPV4", compatibles avec ledit protocole "IPV6", par l'exécution d'une étape de conversion d'adresses conforme au protocole dit "6-to-4".

- 5      4. Procédé selon la revendication 1, caractérisé en ce que ladite étape de chiffrement est effectuée conformément au protocole dit "IPSec", utilisé avec le mécanisme dit "EPS" d'authentification de sources d'information, en mode dit "tunnel", de manière à obtenir des échanges de données sécurisées entre lesdites entités interconnectées ( $U_1$ , 36a-36b, 37a-37d).
- 10     5. Procédé selon la revendication 4, caractérisé en ce que, ladite première entité étant un utilisateur ( $U_1$ ) dudit premier système (4, 20), il comprend une étape d'authentification dudit utilisateur ( $U_1$ ) et en ce que ladite adresse "IP" est utilisée comme donnée d'identification de cet utilisateur ( $U_1$ ).
- 15     6. Procédé selon la revendication 5, caractérisé en ce que lesdites communications s'effectuant en mode paquets de données, lesdites données d'identification d'utilisateur ( $U_1$ ) sont présentes, sous forme chiffrée conforme au dit protocole "IPSec", dans chacun desdits paquets de données.
- 20     7. Procédé selon la revendication 1, caractérisé en ce que ledit premier système (4, 20) est connecté à un segment de transmissions sans fil (RTT), en ce que les communications entre ce premier système constituant un système client (4, 20) et ledit second système constituant un système serveur (3, 3') s'effectuent selon le protocole dit "WAP", et en ce qu'il comprend l'implantation dans ledit second système (3, 3') d'au moins une pièce de logiciel constituant un serveur "WAP" (30) et un deuxième pièce de logiciel (32) formant une interface unifiée entre ledit serveur "WAP" (30) et au moins une application (36a-36b, 37a-37d) offrant ses services à ladite première entité ( $U_1$ ), de manière à ce que ledit serveur "WAP" (30) soit intégré en tant que serveur "WEB" dans ledit système serveur (3, 3').

8. Procédé selon la revendication 7, caractérisé en ce qu'il comprend l'implantation dans ledit second système (3, 3') d'un module supplémentaire (35) d'adaptation bilatérale d'interface de structures permettant de supporter des interfaces applicatives (33) utilisées par les serveurs de type "WEB".

5 9. Procédé selon la revendication 7, caractérisé en ce qu'il comprend l'implantation dans ledit premier système (4, 20) d'une pièce de logiciel constituant un client et en ce que cette pièce de logiciel est un navigateur de type "WAP".

10 10. Procédé selon la revendication 1, caractérisé en ce que ledit premier système étant un système mobile (25), il comprend l'attribution au dit premier système (25) d'une adresse temporaire, en ce qu'il comprend une étape de dialogue entre ledit premier système (25) et un organe d'un type dit "home agent" (23), connecté au dit réseau de type Internet (*it*), permettant de corréler à chaque instant ladite adresse permanente, attribuée à ladite première entité ( $U_3$ ), avec ladite adresse temporaire, selon un protocole dit "mobile IPV6 protocol".

15 11. Architecture de système de communication sécurisé entre des première et seconde entités interconnectées via un réseau de type Internet, lesdites entités étant associées à des premier et second systèmes de traitement informatique de données parmi un ensemble de systèmes distribués connectés au dit réseau de type Internet, caractérisée en ce que le dit premier système (4, 20) est un système fonctionnant en mode dit client et ledit second système (3, 3') un système fonctionnant en mode dit serveur, en ce que lesdites première et seconde entités sont des pièces de logicielles (36a-36b, 20 37a-37d) hébergées dans lesdits premier (4, 20) et second (3, 3') systèmes et/ou un utilisateur ( $U_1$ ) desdits systèmes connectés, en ce lesdites entités ( $U_1$ , 36a-36b, 37a-37d) sont associées à des adresses permanentes de type Internet, du type dit "IP", en ce que ledit second système (3, 3') formant serveur comprend au moins une pièce de logiciel (31) formant serveur (30, 25 31) et offrant les services d'au moins une application (36a-36b, 37a-37d) à

30

ladite première entité ( $U_1$ ), et en ce que lesdits premier (4, 20) et second (3, 3') systèmes comprennent une pile protocolaire de communication comportant au moins une couche d'adressage (44, 390) selon ladite adresse "IP" permanente et une couche logique (45, 391) pour l'exécution d'une étape de chiffrement, en mode bout en bout, conforme à un protocole de sécurisation déterminé, de données échangées entre lesdites entités interconnectées ( $U_1$ , 36a-36b, 37a-37d).

12. Architecture selon la revendication 11, caractérisée en ce que ladite couche d'adressage (44, 390) est conforme au protocole "IPV6".

10 13. Architecture selon la revendication 12, caractérisée en ce que ledit réseau de type Internet ( $R$ ) véhiculant des paquets de données conforme au protocole "IPV4", lesdites piles protocolaires desdits premier (4, 20) et second (3, 3') systèmes comprennent chacune une première couche d'adressage (44, 390) selon ladite adresse "IP" au protocole "IPV6" et une seconde couche (46, 392) d'adressage au protocole "IPV4" dont vont être dérivées des adresses compatibles "IPV6" de manière à obtenir des échanges en mode dit "tunnel" ; lesdites couches logiques (45, 391) exécutant une étape de chiffrement (45, 37) en faveur desdits paquets de données échangés entre lesdites entités interconnectées ( $U_1$ , 36a-36b, 37a-37d).

20 14. Architecture selon la revendication 11, caractérisée en ce que lesdites couches logiques (45, 391) pour l'exécution d'une étape de chiffrement sont conformes au protocole dit "IPSec", utilisé avec le mécanisme dit "EPS" d'identification de sources d'information, en mode dit "tunnel", de manière à obtenir des échanges de données sécurisées entre lesdites entités interconnectées ( $U_1$ , 36a-36b, 37a-37d),

25 15. Architecture selon la revendication 11, caractérisée en ce que ledit premier système (4, 20) est connecté à un segment de transmissions sans fil ( $RTT$ ), en ce que les communications entre ce premier système (4, 20), constituant un système client, et ledit second système (3, 3'), constituant un système

serveur, s'effectuent selon le protocole dit "WAP", et en ce que ledit second système (3, 3') comprend au moins un premier module constituant un serveur "WAP" (30) et un deuxième module (32) formant une interface unifiée entre ledit serveur "WAP" (30) et au moins une application (36a-36b, 37a-37d) 5 offrant ses services à ladite première entité ( $U_1$ ), de manière à ce que ledit serveur "WAP" (30) soit intégré en tant que serveur "WEB" dans ledit système serveur (3, 3').

16. Architecture selon la revendication 15, caractérisée en ce que ledit second système (3, 3') comprend au moins un module supplémentaire (38a-38b) de 10 conversion bilatérale de paquets de données de structures conformes aux dits protocoles "WEB" ou "WAP".

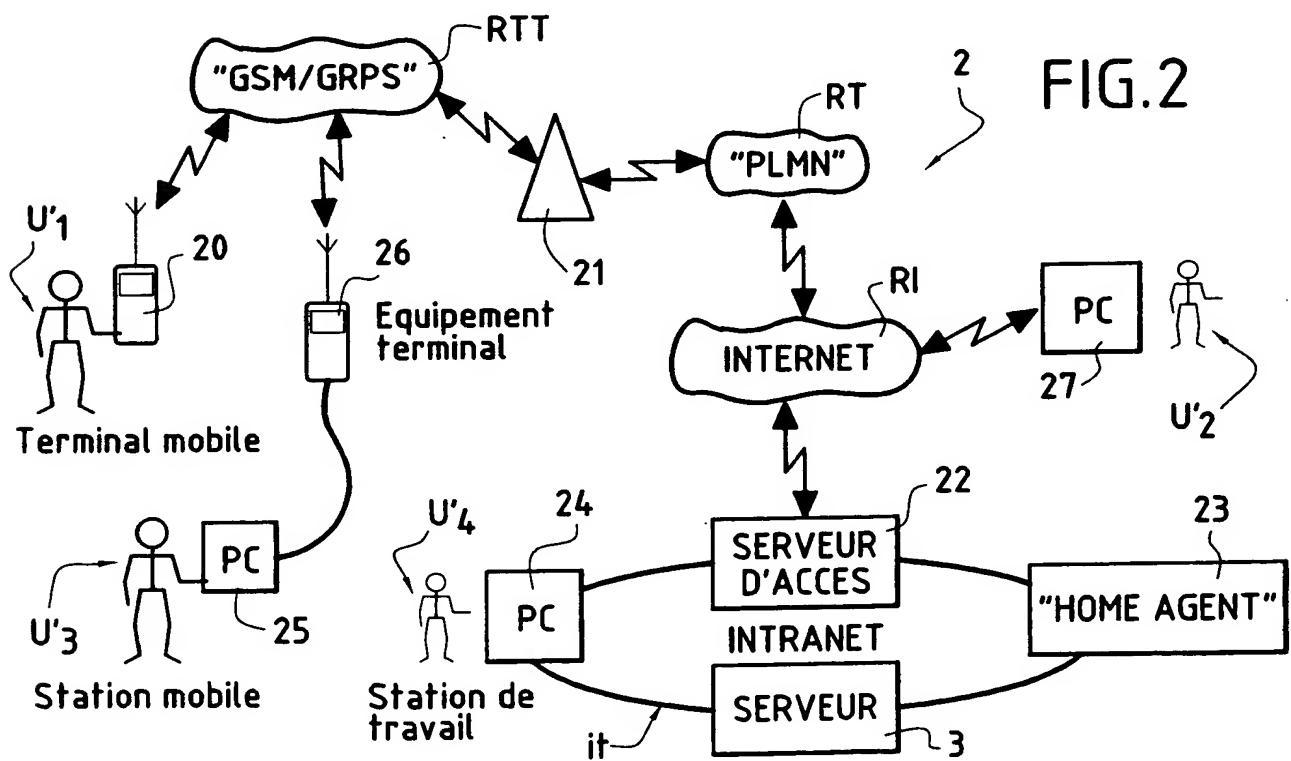
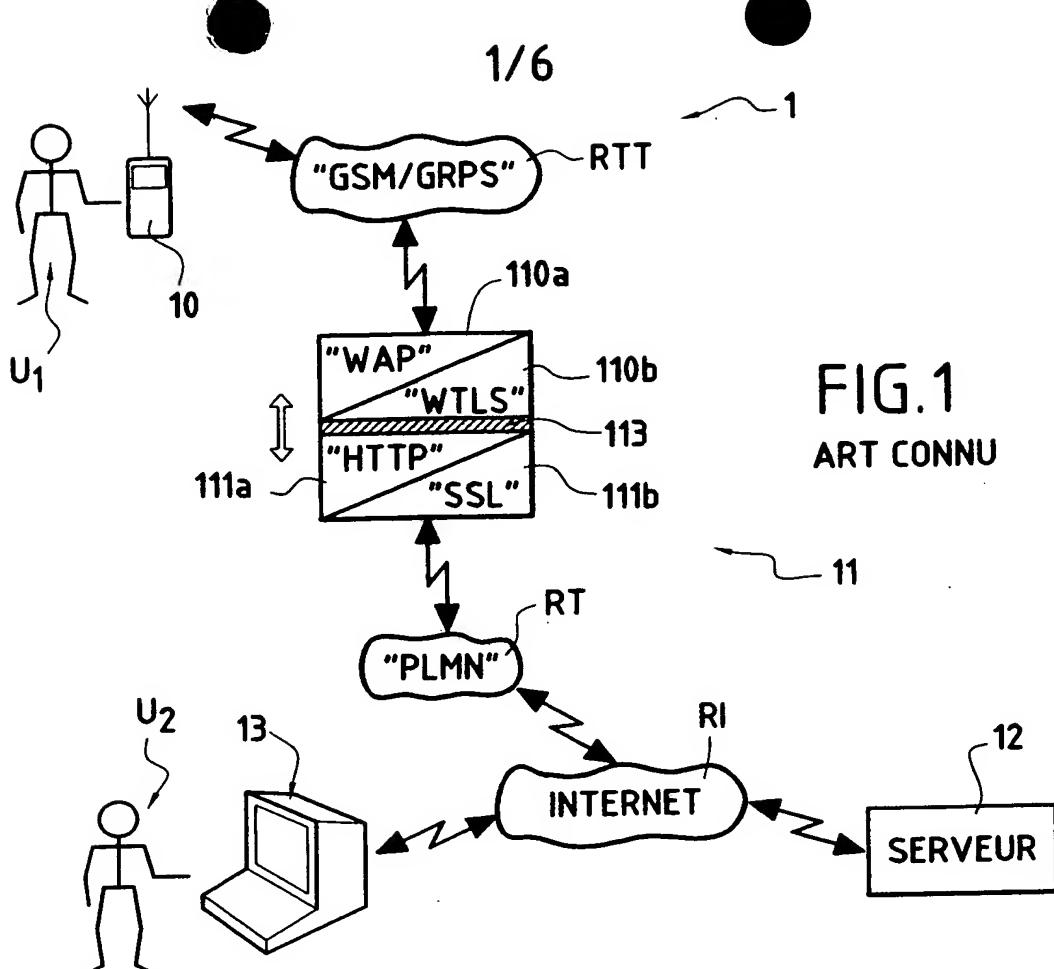
17. Architecture selon la revendication 15, caractérisé en ce que ledit premier système est un terminal de téléphonie mobile (20, 4) à la norme dite "GSM", en ce qu'il comprend un navigateur de type WAP constituant un client, et en 15 ce qu'il comprend un écran de visualisation pour l'affichage de pages en langage du type dit "WML".

18. Architecture selon la revendication 15, caractérisé en ce que ledit premier système est un terminal de téléphonie mobile à la norme dite "GPRS" et en ce qu'il comprend un navigateur de type Internet constituant un client, et en 20 ce qu'il comprend un écran de visualisation pour l'affichage de pages en langage du type dit "WML".

**ABREGE****Procédé et architecture de système de communication sécurisé entre deux entités connectées à un réseau de type Internet comprenant un segment de transmissions sans fil**

L'invention concerne un procédé et une architecture de communication sécurisée entre deux entités ( $U_1$ , 36a) associées à un système (10, 3') et interconnectées à un réseau Internet ( $RI$ ,  $R$ ) comprenant un segment de transmissions sans fil ( $RTT$ ). Les entités sont des applications logicielles (36a) hébergées par les systèmes (3') et/ou des utilisateurs ( $U_1$ ) de ces systèmes (10). L'un des systèmes est un terminal (10) en technologie "WAP" connecté au segment de transmissions sans fil ( $RTT$ ), constituant un système client, l'autre un système serveur (3'). Une adresse permanente réseau est attribuée aux deux entités ( $U_1$ , 36a), de façon préférentielle conforme au protocole "IPV6". Les systèmes serveur (3') et client (10) comprennent une pile protocolaire de communication comprenant des niveaux d'adressage "IP" et de sécurisation de bout en bout, de façon préférentielle conformément au protocole "IPSec" qui assure des services d'authentification de confidentialité et d'intégrité. Le système serveur (3') comprend couche logique supplémentaire (32) permettant à un serveur "WAP" intégré, de disposer d'interfaces applicatives identiques à celles utilisées communément par les serveurs "WEB".

**FIGURE 9**



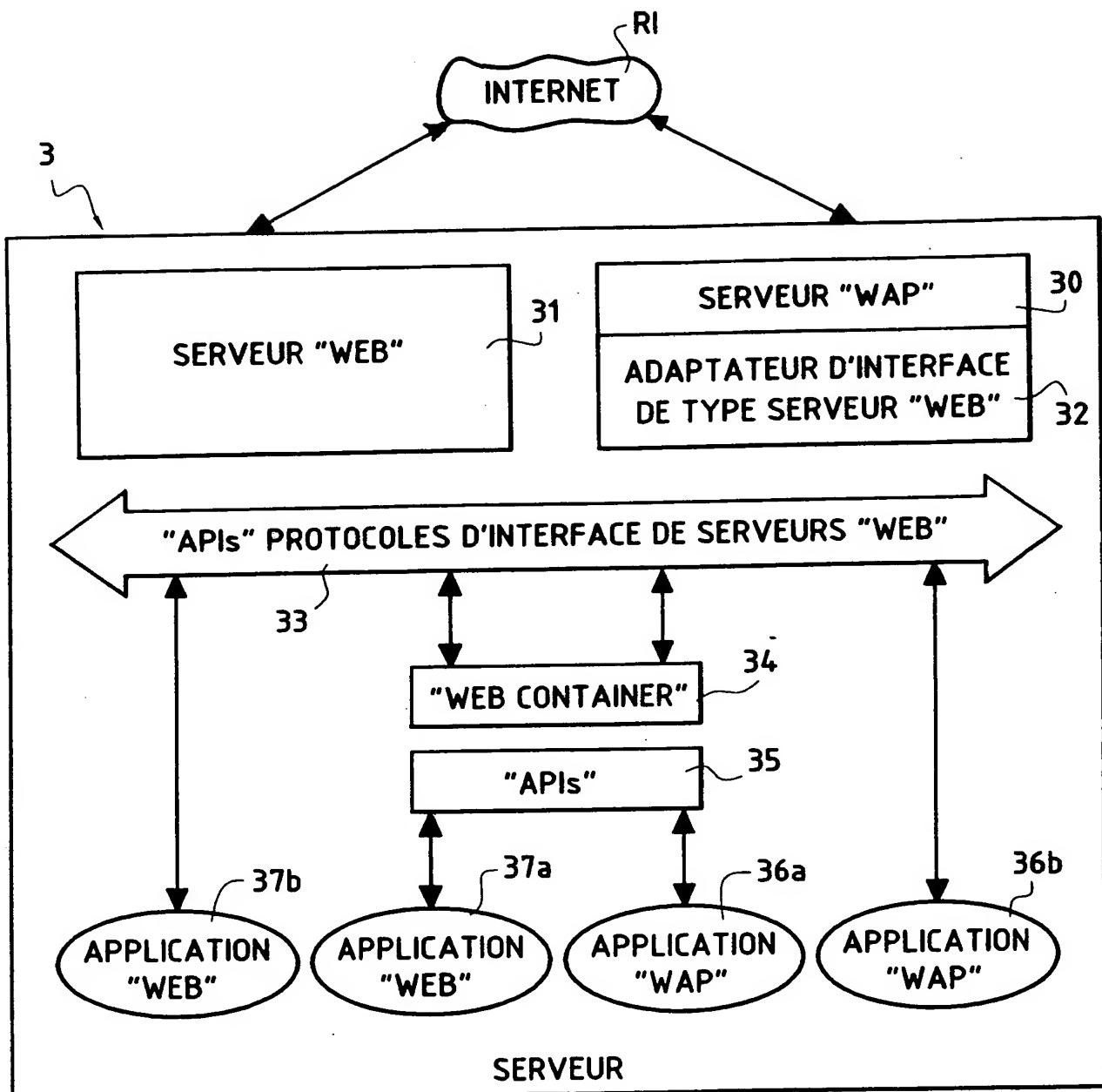


FIG.3

3/6

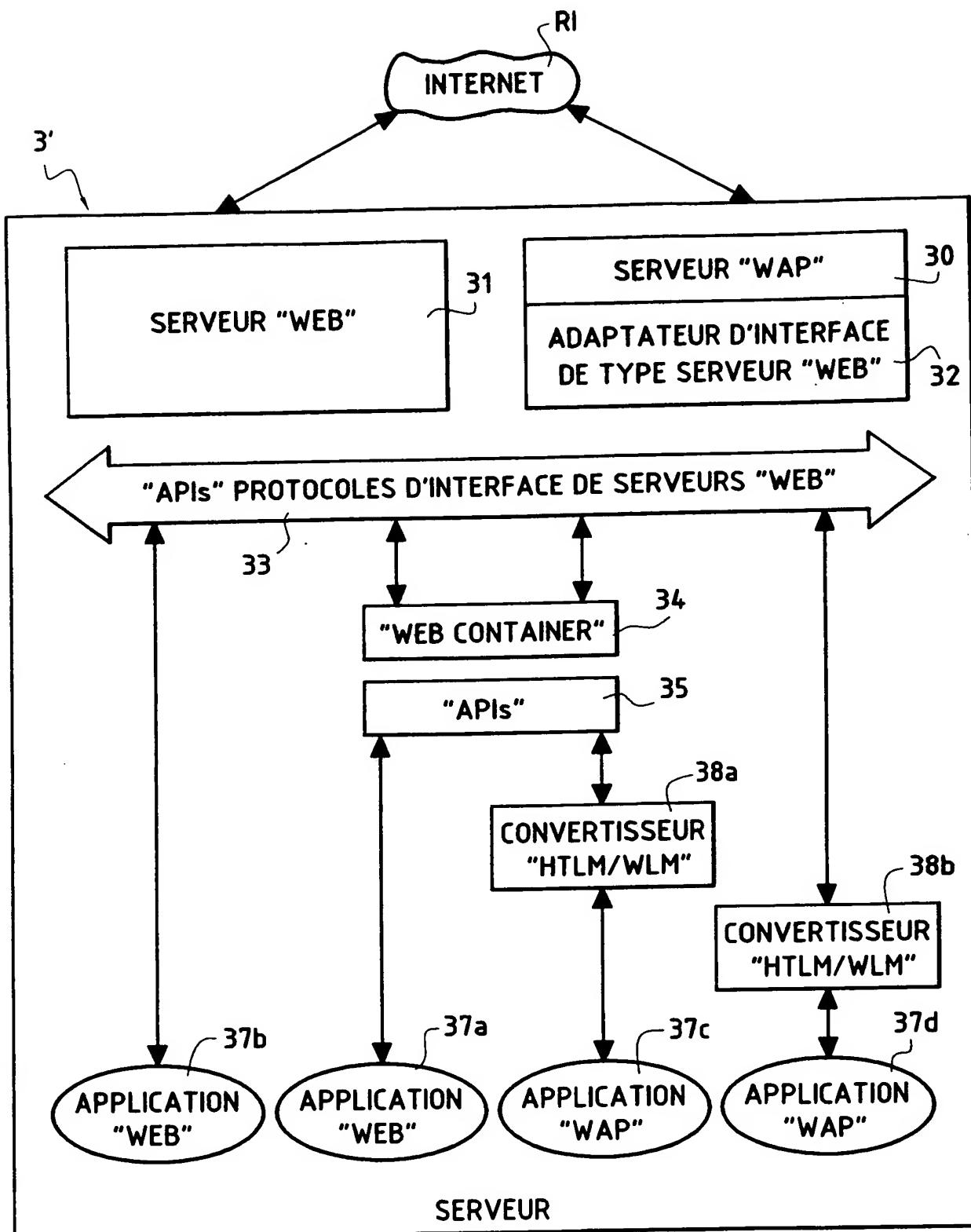


FIG.4

FIG.5

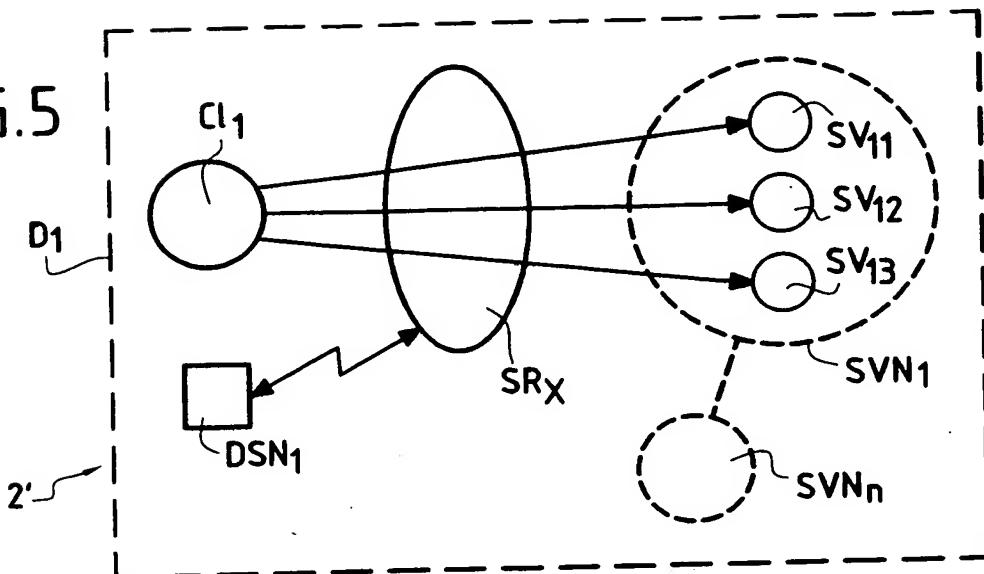


FIG.6

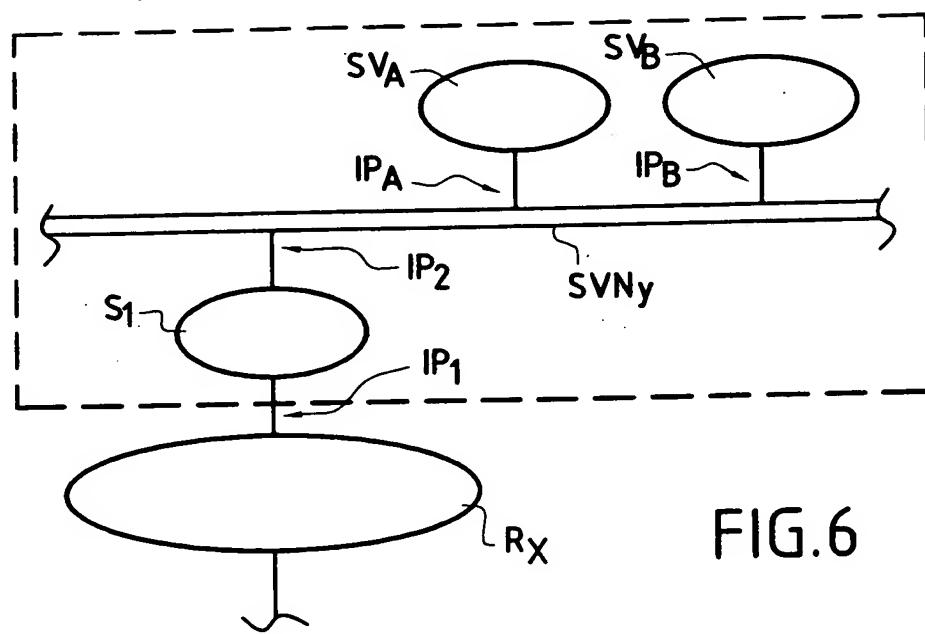


FIG.8

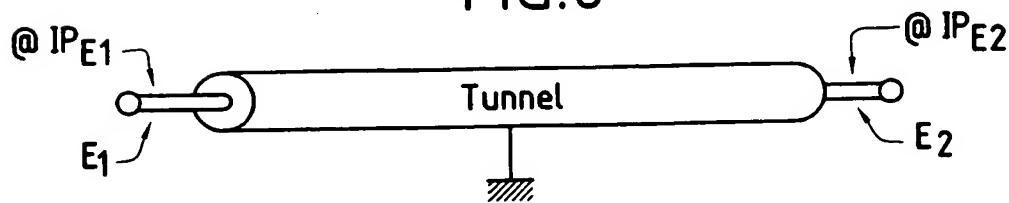


FIG.9

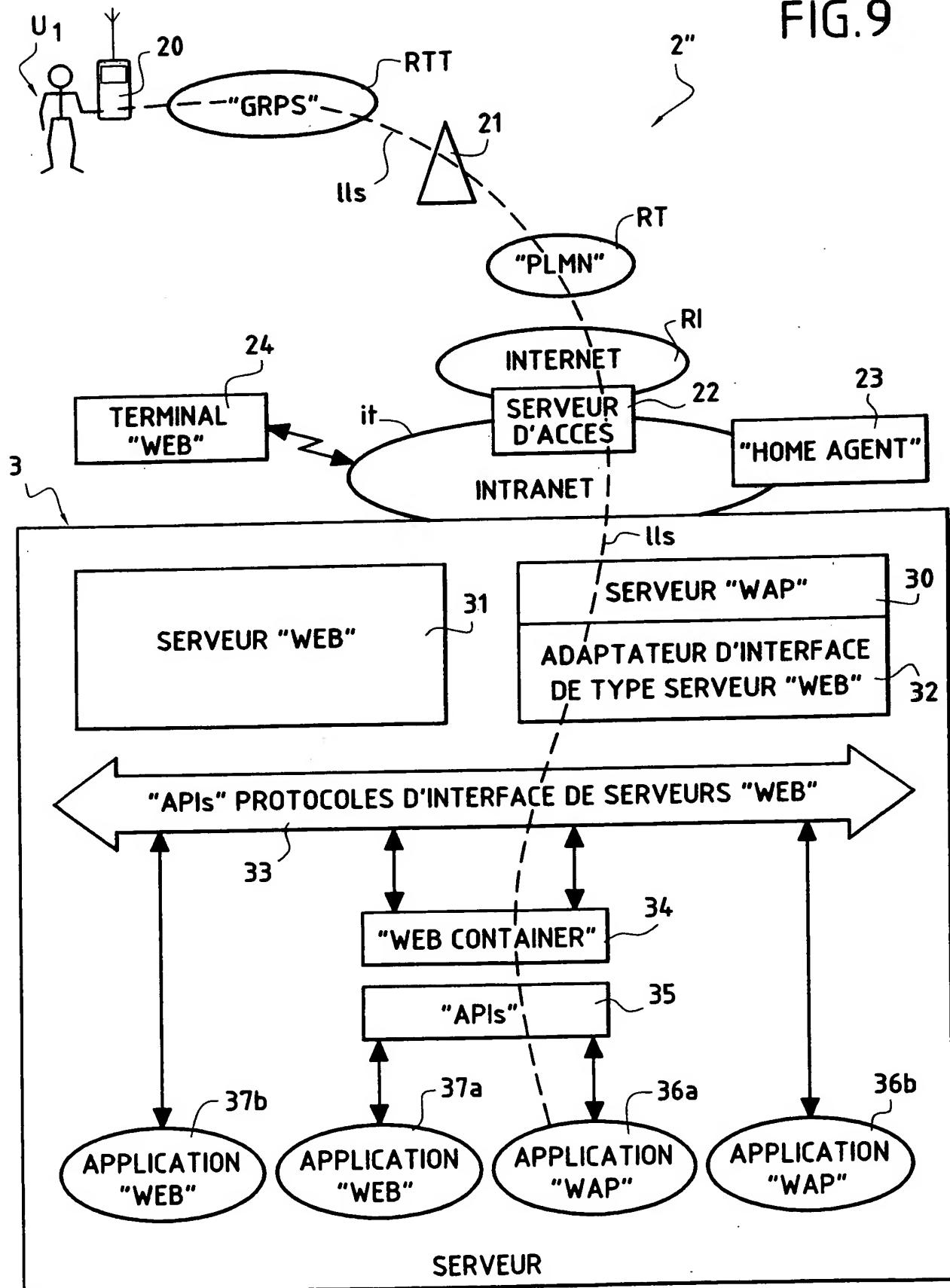
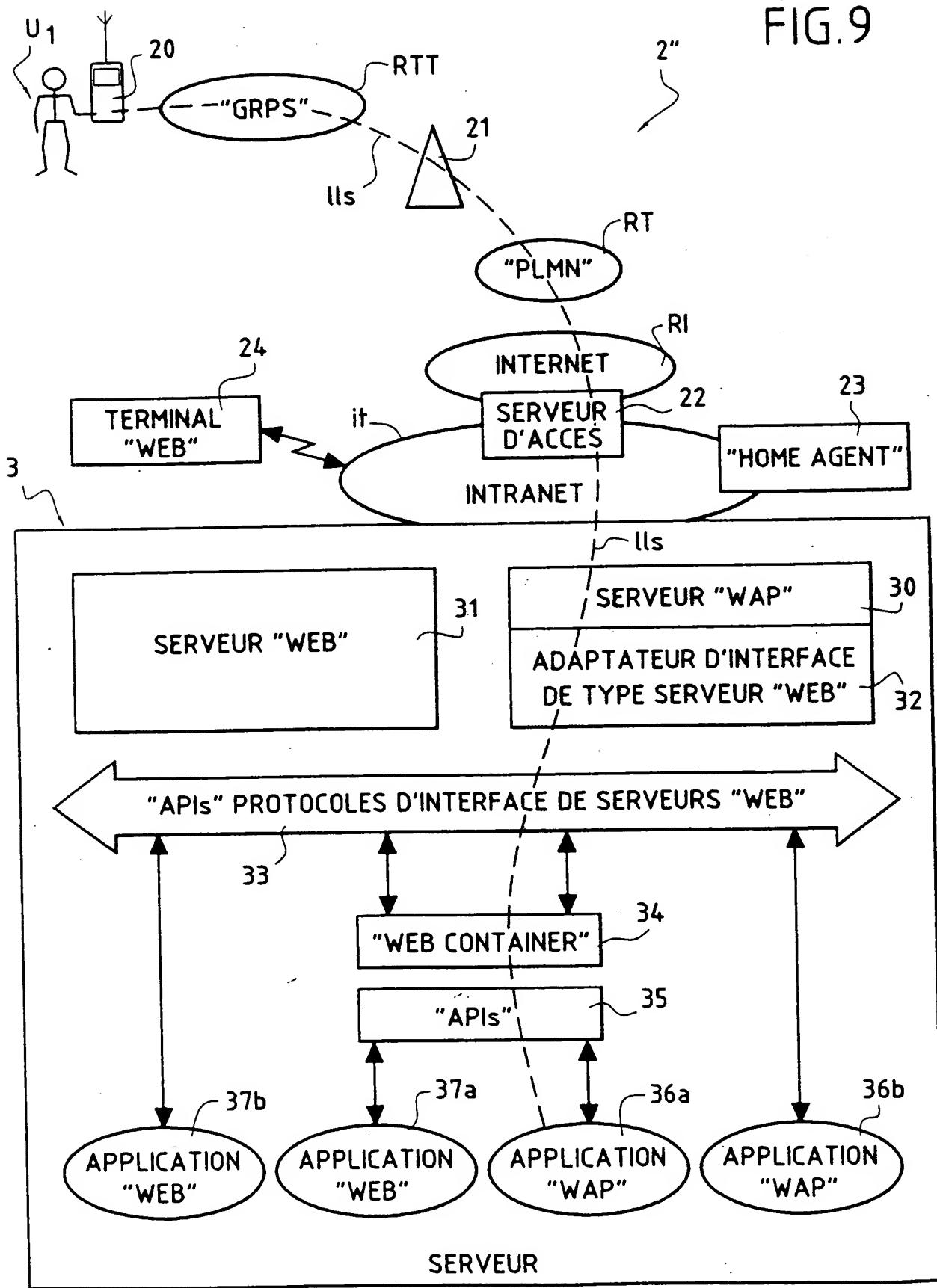


Figure de l'abrégé

FIG.9



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**



Creation date: 10-15-2004

Indexing Officer: ATHUYA - AUNG THUYA

Team: OIPEBackFileIndexing

Dossier: 10048057

Legal Date: 04-12-2002

No.	Doccode	Number of pages
1	M903	2

Total number of pages: 2

Remarks:

Order of re-scan issued on .....